Device Authentication and Consumer Verification Techniques for Mobile In-App and Remote Payments

Version 1.0

March 2023

U.S. Payments Forum
544 Hillside Road
Redwood City, CA 94062

www.uspaymentsforum.org

About the U.S. Payments Forum

The U.S. Payments Forum is a cross-industry body that brings stakeholders together on neutral ground to enable efficient, timely and effective implementation of emerging and existing payment technologies. This is achieved through education, guidance and alternative paths to adoption. The Forum is the only non-profit organization whose membership includes the whole payments ecosystem, ensuring that all stakeholders have the opportunity to coordinate, cooperate on and have a voice in the future of the U.S. payments industry. The organization operates within the Secure Technology Alliance, an association that encompasses all aspects of secure digital technologies.

EMV® is a registered trademark of EMVCo, LLC in the United States and other countries around the world.

Executive Summary

Payment authentication and verification processes are influenced, in part, by the flow of consumer preferences. As more commerce began taking place remotely via online and mobile in-app channels, fraudsters increasingly shifted their attention toward these avenues, and card-not-present (CNP) fraud became more prevalent. The escalation of CNP fraud attempts can also be attributed to increased security in the card-present space brought on by the payments industry's migration to EMV.

Merchants, acquirers, and other payment stakeholders are working to strengthen their digital payment authentication and verification strategies in response to the increasingly sophisticated fraud landscape.

In developing this white paper, the U.S. Payments Forum aims to:

- Provide a comprehensive reference point for payments professionals to increase their understanding of available authentication/verification techniques and tools, their evolution, and standards
- Address potential challenges to the broad implementation of these enhanced authentication/verification tools and techniques
- Promote the adoption of best practices for preventing CNP and other digital payments fraud and increasing digital payment security through a layered approach to authentication/verification

The payments authentication and consumer verification techniques described in this document have been categorized into four segments for ease of access, beginning in section two of the document.

The categories are Consumer Verification, Device Authentication, Risk-Based Authentication (RBA), and Analytics and Familiarity Signals.

In total, this white paper explores 19 techniques which are briefly described below. The applicability, features, associated risks, consumer impact, implementation considerations, maturity, standards, and relevant statistics of each technique are explored in greater detail in sections two through five of the document.

Consumer Verification

2.1 Static Password - A combination of typically eight or more letters, numbers, and special characters. The static password is the most used authentication technique and the least expensive to implement, but often the easiest for fraudsters to exploit.

2.2 Knowledge-Based Authentication (KBA) – A means of authenticating end users by asking "shared secret" questions only the actual person should know. KBA questions are either static (preset at the time of account setup) or dynamic (multiple-choice questions gleaned from databases that include credit and/or demographic data).

2.3 Out-of-Band Authentication (OOB) – A method which provides real-time authentication for network-based (internet and mobile) transactions using a communication channel different from the channel used by all the other messages and data from a device to reduce fraud. Push notifications and one-time passcodes are both examples of OOB authentication.

2.4 Mobile Public Key Infrastructure (PKI) for Push-Based Authentication – A technique that uses cryptography to secure the authentication communication channels during push-based authentication. Push-based authentication validates login attempts by sending access requests via out-of-band notification to an associated mobile device. In mobile PKI systems the communication is encrypted bi-directionally (end-to-end) between the application and a secured authentication service.

2. 5 Virtual Card Authentication – A method which enables consumers or small businesses to generate virtual card numbers to make online purchases in lieu of the real PAN with which it is associated. The cardholder creates a temporary or one-time-use card number, with a security code and expiration date, linked to an existing card PAN.

2.6 Consumer Device Cardholder Verification Method (CDCVM) – An authentication method by which a consumer enters a passcode, password, pattern, or a biometric such as fingerprint, iris, voice or facial recognition on their mobile device.

2.7 EMV Secure Remote Commerce (SRC) – A specification created by EMVCo for click-to-pay which, at its core, focuses on consumer authentication as distinct from cardholder authentication. With SRC-compliant checkout services, users enroll their payment information with the service through their merchant or their card issuer, which then facilitates data transmission between the merchant, issuer, and other parties in the payment process.

2.8 Biometrics – A method for digitally verifying a person's identity through physical or behavioral means. This includes, but is not limited to, fingerprint scanning, facial recognition, iris scanning, voice recognition, or analyzing familiar keystroke patterns during the payment transaction process. Biometric capture can be either active or passive, and physical or behavioral.

2.9 FIDO (Fast Identity Online) – A series of freely available open technical standards created by the FIDO Alliance that utilize on-device public key cryptography to authenticate a user to an online service. The FIDO Alliance aims to replace traditional on-server password authentication with a possession-based public-private key pair similar to that used by EMV card chips.

2.10 W3C (World Wide Web Consortium) WebAuthn API – An API that simplifies the ability of a relying party, such as a web service, to integrate strong authentication into applications using support built into all leading browsers and platforms. Allows web services to offer their users strong authentication with a choice of authenticators such as security keys or built-in platform authenticators such as biometric readers, instead of just a username and password.

Device Authentication

3.1 Dynamic Cryptogram – A cryptogram generated using secret keys stored in a payment device during EMV chip transactions. Information presented from debit or credit card data stored in the mobile wallet and the terminal are leveraged to create a one-time-use dynamic cryptogram which is used by the issuer to authenticate the payment device.

3.2 MNO Risk Scoring, Phone Number Validation, Device Binding and MNO Intelligence – A series of techniques linked to the mobile device that can be used for remote enrollment of payments to validate the user, and as MFA factors. These techniques capture data about/from the consumer or the consumer mobile device to validate against existing attributes stored in the mobile network operator (MNO) database.

Risk-Based Authentication (RBA)

4.1 Adaptive Authentication – A dynamic form of RBA that selects appropriate authentication factors depending on a user's risk profile and tendencies, as well as specific transaction data (e.g., amount). It evaluates multiple parameters, which may include characteristics of the user device, browser, and other attributes; malware detection; geolocation; IP address; consumer use of the mouse and/or keyboard; or other behaviors displayed by the consumer.

4.2 EMV 3-Domain Secure (3DS) – A global risk-based secure messaging protocol that consists of three domains: merchant/acquirer domain, issuer domain, and interoperability domain. 3DS enables issuers to authenticate consumers in real-time during an online or mobile-initiated transaction to reduce fraud and cart abandonment, improve approval rates, and accelerate growth in ecommerce.

4.3 Identification and Verification (ID&V) and Provisioning – A critical part of the provisioning process which ensures that the consumer is the legitimate owner of the payment credentials before a payment token is created and provisioned to a mobile wallet. Examples of ID&V methods include an account verification message, PAN-based risk score assessment, and one-time password.

Analytics and Familiarity Signals

5.1 Predictive Analytics – A process of using analytics to make predictions based on data. This process uses data along with analysis, statistics, and machine-learning techniques to create a predictive model for forecasting future events, behaviors, or most likely outcomes (e.g., potential fraud occurrences).

5.2 Machine Learning (ML)/Artificial Intelligence (AI) for Authentication – AI combines data, algorithms, and computing power to act like a computer with human intelligence. ML is a subset of AI that can be trained through the input of data to make decisions, similar to how a human would respond, but with the ability to act on patterns too complex for humans to identify. Machine learning creates algorithms that process large datasets with many variables and helps find hidden correlations between user behavior and the likelihood of fraudulent actions, among other things.

5.3 Device Familiarity, Risk and Attack Signals – A set of attributes or events originating from a mobile device that can be used to assess the security of an authentication session. These signals can be leveraged to add contextual information for user authentication by providing additional assurance that the authenticating user is valid.

This white paper was created by the members of the U.S. Payments Forum's Mobile and Touchless Payments Working Committee. Its purpose is to provide the industry with a coordinated, in-depth reference point to establish best practices for the implementation of mobile-initiated ecommerce/CNP fraud reduction techniques and tools. It imparts information that will empower payments stakeholders to ask informed questions of solution providers during their continuous journey toward the elimination of payments fraud. In order to mitigate risk in today's complex cybercrime landscape, the payments industry is encouraged to consider a multi-layered approach to authentication. The techniques described in this white paper provide different options for mitigating digital/mobile CNP fraud, depending on the specific circumstances, e.g., payment method, use case, level of risk, etc.

Contents

Figures

1. Overview

As the security of card-present transactions increased fraud shifted to remote channels. Merchants, acquirers, and others are working to strengthen their digital payment authentication and verification strategies. Among other things, this often involves replacing or augmenting weaker authentication/verification methods, such as passwords, with other, newer tools and techniques.

The goals of this white paper are two-fold:

- To educate and inform industry stakeholders (merchants, issuers, processors/acquirers, wallet providers, payment networks, mobile payment platform providers, and consumers) about payment authentication/verification techniques and tools, their evolution, and standards
- To promote broader implementation and adoption of best practices for digital payments

The white paper documents the current landscape of available authentication techniques and tools collected through industry research, input from project team subject matter experts, and interviews with industry stakeholders.

The U.S. Payments Forum project team identified and reviewed different techniques and tools that can improve security for mobile in-app and ecommerce remote payments, relating to both device authentication and consumer verification. For each technique, the white paper includes a high-level description of the relevant verification techniques, the current stage of development, implementation considerations, and use (including examples of industry standards and available statistics). The project team also describes challenges to broad implementation/adoption of enhanced authentication and verification tools.

1.1 Project Scope

The scope of this white paper includes mobile in-app remote/card-not-present (CNP)/mobile browser payments and wallets, along with their related authentication and consumer verification methods. In-person/face-to-face mobile payments, mobile transit payments, person-to-person payments, and any payments NOT initiated on a mobile device were out of scope for this white paper.

The white paper covers 19 techniques in four categories: consumer verification, device authentication, risk-based authentication, and familiarity signals.

Category	Authentication Technique
Consumer Verification	Static Password
	Knowledge-Based Authentication (KBA)
	Out-of-Band One-Time PIN or Passcode
	Mobile PKI for Push-Based Authentication
	Virtual Credit Card Authentication
	Consumer Device Cardholder Verification Method (CDCVM)
	EMVCo Secure Remote Commerce (SRC)
	Behavioral Biometrics
	Physical Biometrics
	Fast Identity Online (FIDO)
	W3C WebAuthn
Device Authentication	Dynamic Cryptogram

Category	Authentication Technique
	MNO Risk Scoring, Phone Number Validation, Device Binding, MNO Intelligence
Risk-Based Authentication	Adaptive Authentication
	EMV 3-Domain Secure 2.0 (EMV 3DS)
	Identity and Verification (ID&V) and Provisioning
Familiarity Signals	Predictive Analytics
	Machine Learning/Artificial Intelligence
	Device Familiarity, Risk and Attack Signals

The white paper follows a common outline for each technique:

- Definition/description
- Applicability (to payment type)
- Technique features
- How the technique works
- Risks associated with technique
- Consumer impact/level of friction
- Implementation considerations
- Maturity and effectiveness of technique
- Applicable industry standards
- Publicly available statistics on implementation and usage

Note that the technique discussions are intended only to provide high-level snapshots to help familiarize readers with factors that may be relevant when assessing the applicability of the techniques described. Readers are cautioned that applicability of a given technique may depend on specific facts and circumstances, including the nature and systems of the stakeholder in question. As a result, the white paper may not include, and does not attempt to attempt to address, all factors that may be relevant, including but not limited to, applicable risks, implementation considerations or consumer impacts. Readers are advised to consult their payment professional advisors, the relevant payments industry stakeholders with whom they interact, and other sources for more detailed information about each technique.

1.2 Security Approach

In general, industry best practice is to use a layered approach ("defense in depth") for security and fraud mitigation. Using a layered approach, security can be improved by pairing common yet more vulnerable techniques, such as static passwords, with multi-factor authentication (MFA), including one-time passcodes (OTPs) and other techniques.

While passwords or other older forms of authentication continue to be used, pairing these with other techniques using a layered approach will prevent passwords from being a single point of security failure. Some techniques, such as CDCVM, may provide higher certainty on the validity of the consumer verification. Risk-based authentication deploys and assesses multiple authentication layers, including behavioral biometrics,[1] for additional protection.

[1] Behavioral Biometrics, International Biometrics+Identity Association, May 2017

In many cases KBA is also used as part of multi-factor authentication, where other security processes such as IP checking are used. The number of correct vs. incorrect answers to a KBA challenge can also yield a risk score to be included in risk-based authentication. Even dynamic KBA should be coupled with a comprehensive fraud prevention platform to quickly pinpoint suspicious behavior and escalate to a higher level of verification based on risk. According to the Identify Management Institute, "In systems designed to operate on a contextual basis, KBA is useful to fall back on when users can't meet the requirements for other forms of authentication. Using KBA along with behavior monitoring incorporates patterns of users' actions into the authentication process, allowing for termination of sessions or denial of access should unusual behaviors be detected."[2]

Other techniques, such as Secure Remote Commerce/SRC, are, by definition, layered approaches as they orchestrate multiple participant data sources and aggregate authentication and assurance data during a CNP checkout. SRC uses consumer, cardholder, card, and device authentication as well as binding, encompassing a variety of implicit authentication techniques.

1.3 Information Access

The project team also considered factors such as:

- How far along the payment transaction value chain does the information travel?
- What is the role of each party who touches the data in the process (value chain)?
- Who authenticates data, who matches data, who validates the transaction, and who receives results (among other questions)?

Some techniques can be used independently by any stakeholder in the payments value chain, including static passwords, one-time passcodes, behavioral biometrics and KBA. Typically, nothing about the authentication result would travel down the value chain. The authenticator and potentially its service provider validate the passcodes, biometric result, or secret question. No other stakeholder can access the data.

Other techniques pass a validation result down the value chain. For example, with CDCVM, the global networks pass the consumer verification result from the payment terminal through the network to the issuer for verification.[3] The issuer will then verify the information received in the authorization message before the transaction is authorized.

[2] Knowledge-Based Authentication Weaknesses, Identify Management Institute

[3] This applies only to Global networks. Domestic networks are not allowed to receive CDCVM.

2. Consumer Verification

Consumer verification techniques range from some of the earliest security measures ever used, such as static passwords and secret questions, to techniques at the cutting edge of technology, such as behavioral biometrics. Current activity has been to augment the more vulnerable techniques with additional and "out-of-band" security measures such as one-time passcodes and other push-based authentication techniques. However, the goal of new consumer verification techniques is a future in which authentication is more foolproof and completely seamless to the consumer, by shifting to passwordless authentication with biometrics and Fast IDentity Online (FIDO).

2.1 Static Password

2.1.1 Definition/Description

Static passwords are a combination of typically eight or more letters, numbers, and special characters.

The paradox of passwords is that the easier it is for a user to remember, the easier it is for an attacker to guess. However, passwords that are difficult to remember may reduce the security of a system since they may either be written down or reused across multiple accounts. Password reuse is the single biggest security flaw with the use of passwords. Fernando Corbato, the man who pioneered the use of the password online, has described the situation as a "kind of nightmare."[4]

2.1.2 Applicability

Static passwords as an authentication technique could apply to any payment type. This technique is applicable to the mobile browser, and in-app. Static passwords can be used by the issuer, or processor on its behalf (issuer), and the merchant/acquirer.

The static password is the most used authentication technique and least expensive to implement.

2.1.3 Technical Features

Passwords may be sent across encrypted channels, most commonly Transport Layer Security (TLS), formerly Secure Socket Layer (SSL).

2.1.4 How the Technique Works

Some systems store passwords in plain text; others more securely store passwords in encrypted form. More secure systems don't store passwords at all, instead comparing password entries with a hashed version (a mathematical algorithm that does a one-way mapping to a new value).

To prevent bystanders from seeing the password, it is typically masked as it is typed in. Some systems enforce a time-out of several seconds and/or a small number of failed password entry attempts (e.g., three). This is intended to foil the rate at which an attacker can submit guesses.

The password (or the hashed version of it) may be passed over the network in plain text, which is subject to snooping, or over encrypted channels. The system must provide a way for the user to change the password in the case of compromise.

[4] The Future of Authentication: Why do passwords still exist?, Raconteur, 2020

Many organizations and systems enforce changing passwords on a periodic basis, but there is some debate about the effectiveness of this policy. The National Institute of Standards and Technology (NIST) has changed its advice on mandatory password resets stating that the practice is ineffective and that preventing the use of old, weak, or similar passwords is more important.[5]

2.1.5 Risks Associated with the Technique

Over 22 billion records were exposed in data breaches in 2021.[6] Since many data breaches have targeted username and password, static passwords are considered one of the greatest vulnerabilities in any computer system, calling for additional layers and types of authentication.

Despite Bill Gates' prediction of the demise of passwords as far back as 2004, the password reuse problem is a ticking time bomb: a 2019 survey by Google revealed that 65% of people use the same password for some or all accounts.[7]

In 2013, Google[8] released a list of the most common password types, considered insecure because they would be easy to guess, especially after researching an individual on social media. The problematic passwords included names of a pet, child, family member, or significant other; anniversary dates and birthdays; birthplace; name of a favorite holiday; something related to a favorite sports team; and the word "password." Many seemingly innocent quizzes and challenges on Facebook may be looking for this type of information.

There are five ways hackers steal passwords:

- **Theft of a database** containing login credentials
- **Phishing, social engineering, or man-in-the-middle attack** using a fake email to trick consumers into sharing credentials
- **Keyloggers, browser injections and other malware** to capture credentials
- **Password attacks and password spray,** including brute force, attempt of common passwords and automated attacks designed to crack or guess passwords
- **Local discovery** with physical search or Wi-Fi scanning to discover credentials

Stolen credentials are then used for "credential stuffing," automated testing of stolen usernames and passwords at other sites with the intent of taking over a large set of accounts all at once.[9,10]

2.1.6 Consumer Impact/Level of Friction

If people are asked to remember many passwords, they just give up.[11] "Security fatigue" – weariness or reluctance to deal with computer security – drives password reuse as the path of least resistance**.** Statistics vary, but one source reported that some people had as many as 85 passwords for all their accounts in 2020.[12]

---

[5] The Password Reuse Problem Is A Ticking Time Bomb, HelpNetSecurity, 2019
[6] Over 22 Billion Records Exposed in 2021, Security Magazine, 2022
[7] Online Security Survey, Google/Harris Poll, 2019
[8] Google Reveals the 10 Worst Password Ideas, TIME.com, 2013
[9] How Hackers Steal Your Reused Passwords: Credential Stuffing, Dashlane, 2017
[10] Your Pa$$word Doesn't Matter, Microsoft, 2019
[11] 'Security Fatigue' Can Cause Computer Users to Feel Hopeless and Act Recklessly, New Study Suggests, NIST, 2016
[12] 55 Important Password Statistics You Should Know: 2022 Breaches & Reuse Data - Financesonline.com, Cnet, 2020

Users are advised to get a password management app and eliminate all duplicate passwords.[13] However, it is important to point out these apps are not foolproof. Some may be subject to phishing and brute force attacks; some use weak matching criteria or mismatched URLs for autofill suggestions.[14] Following the recommendations of so-called "experts" –when even those recommendations have weaknesses– further contributes to "security fatigue."

A problem for stakeholders is not to make authentication too challenging. Despite the headache associated with passwords, consumers are accustomed to using them. Implementers must consider whether adding additional friction, such as requiring MFA, would compromise the consumer experience, resulting in a competitive disadvantage. U.S. implementations typically differ from those in the EU, where MFA is required by regulation.

As more purchasing activity moves to the mobile channel, use of biometrics may ultimately result in the elimination of passwords.

2.1.7 Implementation Considerations

A static password requires no back-end server integration and works with most legacy username/password solutions.[15] There are no compatibility issues and no requirements for additional hardware, thus they are cost effective to implement.[16]

2.1.8 Maturity and Effectiveness of the Technique

Passwords are mature. They have been used along with usernames for logging into computer systems since the beginning of the computer age in the early 1960s. Although passwords are widely recognized to be a security vulnerability and a headache for consumers, implementation simplicity keeps them in use vs. other stronger alternatives, like biometrics, which are more complex and expensive. Passwords are easy to use and if compromised, easy to replace.[17]

2.1.9 Applicable Industry Standards

NIST SP 800-63 "Digital Identity Guidelines"[18] provide a detailed set of rules explaining how passwords should be created. It states that passwords should be randomly generated, at least eight characters and up to 64 characters. The password should be a combination of numbers, upper- and lower-case letters and symbols, and not be reused. Further, the password should be verified against known password dictionaries, be used with password managers, have at least 10 password attempts before lockout, and have infrequent password changes. Words, pets, people, places, and adjacent keyboard strings should not be used.[19]

2.1.10 Publicly Available Statistics on Implementations and Use

Most websites use passwords, with an estimated 300 billion active passwords worldwide.[20]

---

[13] The Real Life Risks Of Re Using The Same Passwords, Pixel Privacy, 2017
[14] Security Flaws Found in Popular Password Managers, WeLiveSecurity, 2020
[15] Understanding Core Static Password Features, Yubico, 2018
[16] The Future of Authentication: Why do passwords still exist?, Raconteur, 2020
[17] The Future of Authentication: Why do passwords still exist?, Raconteur, 2020
[18] NIST SP 800-63 Digital Identity Guidelines
[19] Top Ten 2019 Password Security Standards, Liquid Web, 2019
[20] The Future of Authentication: Why do passwords still exist?, Raconteur, 2020

2.2 Knowledge-Based Authentication

2.2.1 Definition/Description

Knowledge-based authentication (KBA) authenticates end users by asking "shared secret" questions only the actual person should know. Typically, the answers are "out-of-wallet," meaning that the information to answer the question is not available in a person's physical wallet.

2.2.2 Applicability

KBA as an authentication technique could apply to any payment type. This technique is applicable to the mobile browser, used primarily to reset a password, and is also used in provisioning. KBA can be used by both the issuer and the merchant/acquirer.

2.2.3 Technical Features

Stakeholders that use KBA (e.g., issuers, merchants, payment service providers [PSPs]) store their proprietary data. They may work with vendors that can access additional data from outside sources to generate dynamic questions. For static KBA, the provider collects, and stores information shared by the consumer at the point of initial contact—usually questions and corresponding answers—and retrieves the data when the consumer comes back to access the account.

To initiate the process for dynamic KBA, a consumer must provide basic identification factors such as name, address and date of birth when creating the account. The issuer checks the data with an identity verification service. After the identity is verified, the issuer's system generates questions in real time from the data records corresponding to the individual identity provided.

2.2.4 How the Technique Works

By selecting questions that only the target individual would know the answers to, systems can verify whether a user is the legitimate owner of an account. KBA questions may be factual (e.g., "What color is your 2002 Honda CRV?") or subjective (e.g., "What is your favorite animal?").

KBA questions are either static (preset at the time of account setup) or dynamic (multiple-choice questions gleaned from databases that include credit and/or demographic data). For static KBA, the user selects the security questions to be asked and inputs the answers to the pre-selected question. Dynamic KBA generates questions in real-time from the data records, often from either credit bureaus or public demographic data; it does not require prior contact with the consumer.[21] Another variation of dynamic KBA for existing consumers is the use of recent transaction data.[22] Typically, the time given for the person to respond, and the number of attempts allowed are limited to prevent answers from being researched.

[21] What is KBA? Knowledge based authentication explained, SIGNix, 2015

[22] The Role of Dynamic Knowledge-Based Authentication in a Digital World, IDology, 2019

2.2.5 Risks Associated with the Technique

According to NIST and other industry stakeholders, KBA is easily compromised and is no longer considered a viable authentication method.[23] Any information known is potentially at risk of being inadvertently shared or stolen. As a result, KBA is vulnerable to numerous compromise methods, including:

- **Simple searches**. Often it takes only a simple search to uncover the answer. Hackers can leverage social media or use other public information to guess the answers to the most common questions as much as 20% of the time.[24] As an example, "mother's maiden name" is available on genealogical web sites.[25]
- **Public database access**. Material for dynamic KBA is from publicly available databases, social media, or other databases such as credit bureaus (that have been breached).
- **Purchase of stolen information**. Information from hacked databases is available for hackers to purchase. A recent phenomenon known as credential stuffing may be used where criminals take entire lists of stolen security answers and test variations against different sites.
- **Data interception**. Answers can be intercepted or stolen and replayed.

2.2.6 Consumer Impact/Level of Friction

90% of consumers think KBA is easy. According to IDology's 2018 Consumer Digital Identity Study,[26] consumers consider KBA as the second most secure form of digital identification, behind biometrics.

Good KBA questions should be those that users can easily remember; however, there are many cases in which a person forgets the KBA answer chosen. KBA systems often are more effective when users are offered canned questions to choose from; requiring users to answer one question is nearly as secure as requiring two answers.[27]

Sometimes asking outdated information can lead to poor consumer experience; for example, asking for a spouse's name if the spouse is deceased could prove somewhat traumatic to a consumer.

2.2.7 Implementation Considerations

KBA is less complicated to implement than other authentication techniques and requires a moderate effort to manage. KBA does not require large upfront costs – it can be implemented via web portal access or API integration.[28] The solution, types of questions, and approval rules must be configured according to the desired strategy, balancing business needs with consumer experience. The most effective dynamic KBA solutions include the ability to:[29]

- Configure approval/pass/fail criteria
- Specify the number of questions and number of multiple-choice answers presented
- Prioritize or suppress question types
- Set time limits for answers
- Limit the number of times a consumer can repeat the questions within a specified time
- Respond when using a new device or location

It is important to note that merchants may have issues with contacting credit bureaus or others to ask for information due to risk, privacy or legal concerns. Legal counsel may also have concerns about privacy and compliance with the applicable data protection regulations.

Implementation of KBA is isolated to whatever party is authenticating the consumer, thus does not require action on the part of any other participant in the ecosystem.

2.2.8 Maturity and Effectiveness of the Technique

KBA has existed for quite some time. While the exact age is unknown, one of the earliest articles on this topic dates back to 2005. Solutions are available from security software vendors and credit bureaus.

2.2.9 Applicable Industry Standards

In 2011, the Federal Financial Institutions Examination Council (FFIEC) recommended the use of dynamic vs. static KBA, however this view has changed. NIST Special Publication 800-63-3 "Digital Identity Guidelines," published in June 2017,[30] specifies that KBA does "not constitute an acceptable secret for digital authentication" in a classic three-factor authentication scheme – something you know, something you have, something you are.

2.2.10 Publicly Available Statistics on Implementations and Use

Static KBA is one of the most widely used methods of identity verification. According to the FIDO Alliance "2017 State of Authentication Report,"[31] static KBA is the second most used authentication method (27%) in the mobile channel (behind password at 100%). Dynamic KBA is fourth (19%) in the mobile channel. Hackers can guess the answers to the most common security questions as much as 20% of the time, and 20% of the answers to security questions are forgotten within six months of account creation.[32]

[23] KBA Alternatives, Jumio

[24] Everybody Knows: How Knowledge-Based Authentication Died, Forbes, 2018

[25] Are knowledge-based authentication systems doing more harm than good?, SearchSecurity, 2007

[26] Knowing Knowledge-Based Authentication, IDology, 2018

[27] Are knowledge-based authentication systems doing more harm than good?, SearchSecurity, 2007

[28] Knowledge-Based Authentication with ExpectID IQ, IDology

[29] Knowledge-Based Authentication, ID Analytics

[30] NIST Special Publication 800-63-3: Digital Identity Guidelines, NIST, U.S. Department of Commerce, 2017

[31] 2017 State of Authentication Report, FIDO Alliance

[32] Everybody Knows: How Knowledge-Based Authentication Died, Forbes, 2018

2.3 Out-of-Band Authentication: One-Time Passcode

2.3.1 Definition/Description

2.3.1.1 OOB Authentication[33]

Out-of-band authentication (OOBA) provides real-time authentication for network-based (internet and mobile) transactions using a communication channel different from the channel used by all the other messages and data from a device. For example, the OOBA message might use a cellular channel, whereas other device messages might use an internet channel. Because OOBA uses different channels, the authentication process can reduce the chance of fraud. Fraudulent users may only have access to one of the channels.

One of the most common applications of OOBA is for online banking transactions. Typically, a consumer performing an online bank transaction logs-in to the banking application with a username and "permanent" password and then receives an SMS[34] message that includes a code via mobile phone. Any hackers or identity thieves that have access to a user's internet connection will not have access to the OOBA one-time PIN or password (OTP), because it was sent over the wireless network, not the internet. This type of authentication is effective only if fraudsters have not gained access to the user's mobile phone or the network that supports it.

2.3.1.2 One-Time Passcode

An OTP is valid for only one login session or transaction and expires after use. It is typically part of a two-factor authentication (2FA) process to provide an extra layer of security for the user when logging in and/or conducting a payment transaction on a computer or mobile device. Although an OTP is only valid for a single use and cannot be reused a second time by anyone, it can be subject to man-in-the-middle (MiTM) attacks.

Different algorithms can be used to generate an OTP. A time-based OTP is commonly used for financial services/payments. Its functionality is highly configurable. The following items can be set for each implementation: length of the OTP code, time of expiry, number of retries. Providers select the requirements for each of these variables based on how tight the controls need to be for the process being authenticated.

2.3.2 Applicability

Financial institutions (FIs), merchants, third-party payment service providers (PSPs) and other industry stakeholders use OTPs to authenticate remote mobile and online payments during enrollment and transaction processes as part of step-up authentication for high-risk or suspicious activity, and to minimize the risk of fraudulent login attempts and stolen passwords or PINs.

2.3.3 Technical Features

Two types of OTPs are used: Hashed Message Authentication Code (HMAC) One-time Password (HOTP) and Time-based One-Time Password (TOTP).[35]

---

[33] OOB authentication ,Techopedia

[34] SMS, "Short Message Service," is an OOB method that sends text messages to mobile phones. An SMS message is typically limited to 160 characters. All major cell phone systems support SMS. SMS Definition .

[35] Advance Authentication User guide- HOTP, Netiq

HOTP is an event- or counter-based algorithm. The counter is stored on the hardware token and must be synchronized with the counter stored on the server that validates the submitted OTP code. A static secret key, known only by the token and the server, and more than one consecutive OTP (generated from the token) can be used to enroll. To authenticate a transaction or sign on, the OTP in the token is compared to the OTP generated in the server. If the OTPs are identical, the transaction or sign-on authentication is successful, and the session can proceed to the next step. The counter in the token increments when the button on the token is pressed, and the counter on the server is incremented only when an OTP is successfully validated.

Because the token and the server can get out of sync, special procedures are needed, with appropriate security, to re-synchronize them.

Generic HOTP tokens follow the related IETF[36] standard, RFC 4226, which covers the algorithm used to generate OTP values, based on the HMAC.[37]

TOTP is a temporary passcode generated by an algorithm that uses the current time of day as one of its inputs. Time-based one-time passwords are commonly used for 2FA, with growing adoption by cloud application providers. The TOTP is valid for a short duration, typically 30 seconds. TOTP is similar to HTOP but uses time instead of a counter. TOTPs do not have the same out-of-synchronization issues as HOTPs.

2.3.4 How the Technique Works

OTP delivery methods include SMS, voice, hard token, soft token, mobile app, and email. When a user logs in to a system (e.g., an issuer or PSP) with username and password, an on-demand OTP is sent to the user via the delivery method the organization has in place. The ubiquity of mobile phones serves as one effective means to send an OTP to a user. OTP delivery options are described below.

- **SMS**. The provider uses SMS to transmit an on-demand OTP to users for authentication during a payment transaction or for enrollment in a new payment service. The user enters the OTP into the system prompt to verify identity and gain access.
- **Email**. The provider sends an on-demand OTP to the user's email, where the user retrieves it and enters the OTP into the system prompt to verify his identity and gain access.
- **Voice**.[38] The OTP is delivered via a phone call to a registered phone number, typically received and confirmed within minutes. Once entered in the device and transmitted to the host, the voice-delivered OTP is compared with the OTP generated on the server. If the OTPs match, the user authenticates successfully. If the user has not registered a phone number in his profile, the voice OTP method will not be enrolled automatically. However, some providers allow users to enroll a phone in the voice OTP method manually.

Time-based -one-time -password (-TOTP), SearchSecurity
OTP (One-Time PIN) Code, Infobip
HOTP vs TOTP: What's the Difference?, Microcosm, July 2018

[36] IETF: Internet Engineering Task Force. The IETF is an open standards organization, which develops and promotes voluntary Internet standards, in particular standards that comprise the Internet protocol suite.

[37] HOTP: An HMAC-Based One-Time Password Algorithm , Tools Left, Dec 2005

[38] Voice OTP, Netiq

- **Hard token**. A hard token is a physical device that generates security codes the consumer uses to authenticate during a logon process. The hardware security token is typically a pocket-sized device with a small screen that generates and displays a single-use, unique multi-digit numeric code (OTP/token), whenever a button on the device is pushed, or every 30 or 60 seconds, depending on the device. To authenticate, the consumer enters the username, password, and code displayed on the token into their mobile device. The OTP token hardens a traditional ID and password system by adding a dynamic credential. Depending upon the vendor, an OTP token will generate a PIN synchronously or asynchronously. Synchronous tokens use a secret key[39] and time to create an OTP. Asynchronous tokens use a challenge-response authentication mechanism (CRAM).[40]
- **Soft token**.[41] Soft tokens generate a dynamic passcode in software to display on the user's device. Soft tokens eliminate the need for another hardware device. However, the risk exists that the software can be hacked or duplicated and used maliciously. One type of soft token is a mobile app. Vendors provide authenticator app solutions that consumers download and apply to certain payment solutions for an additional authentication factor. Some payment providers (e.g., PayPal) offer consumers the option to select 2FA from an authenticator app incorporated into the provider's system, instead of choosing to receive an SMS OTP. (See Figure 1.)

Push notification authentication is another OOBA authentication delivery method. Push notifications are messages that pop up on a mobile device to deliver timely and relevant information to users. They look like SMS text messages or message alerts, but they only reach users who have installed the app associated with the sender of the notification. The user does not have to be in the app or be using their device to receive a push notification. Each mobile platform (e.g., iOS, Android) has its own support for push notifications. The message provider's server pushes the notification text to the iOS/Android push notification. When the user accesses the app, the server registers that device, and sends the notification only to that device.

While push notification is a type of OOBA, it is not considered an OTP. Push notification enables user authentication by pushing the notification directly to a secure application on the user's device, alerting them that an authentication attempt is taking place. Users can view authentication details and approve or deny access, typically by pressing a button. Notifications can be sent in-band or out-of-band, using various communications channels. They authenticate the user by confirming that the device registered with the authentication system – typically a mobile device – is in the user's possession. However, if the device is compromised by an attacker, push notifications are compromised.

[39] OTP security tokens produce a numeric or alphanumeric code to authenticate access to the system or transaction. This secret code changes every 30 or 60 seconds, depending on how the token is configured.

[40] Challenge-response authentication (CRAM) is a family of protocols in which one party presents a question (challenge) and another party must provide a valid answer (response) to authenticate.

[41] One-time password token (OTP token), SearchSecurity

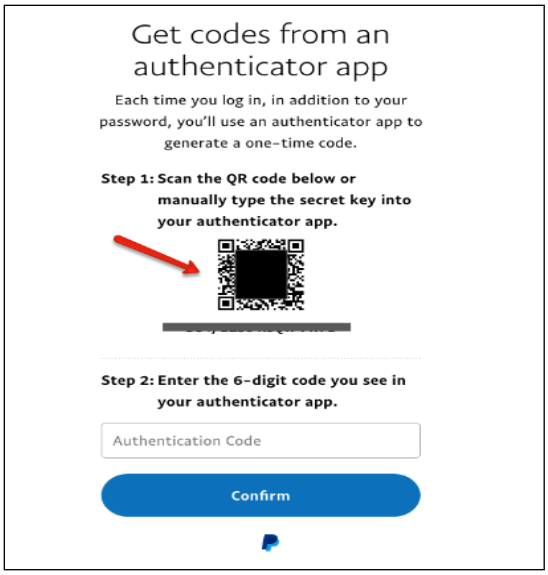

Figure 1. PayPal Authenticator App[42]

2.3.5 Risks Associated with the Technique

Several risks are associated with OOBA and OTPs.

Spoofing and Social Engineering

On-demand delivery methods are susceptible to spoofing, a phishing technique that hackers use to trick consumers into giving them account information or codes by pretending to be a legitimate source. The attacker must already have the username and password to gain access, and then visits the login page and requests a "reset password" 2FA code. The attacker then sends the victim an SMS message or email that appears to be from a legitimate source and says something like: "Suspicious activity has been detected on your account. Respond with the code you received to prevent unauthorized access." If the victim forwards the code, the attacker can gain easy access to the account.

Man-In-The-Middle Attacks

The mobile device is infected by malware that taps into the message on the device that contains the OTP. The attacker must also have the username and password.

Stolen or Intercepted OTPs

NIST does not recommend use of OTPs with SMS delivery. In July 2016,[43] NIST announced that OTPs should no longer be sent to mobile phones via SMS message because OTPs can be easily stolen. NIST also warned that the ability to receive email messages or other types of instant messages "does not generally prove the possession of a specific device," so OTPs also should not be used as OOBA methods. NIST recommends that organizations use more secure authentication methods, such as push notifications, soft OTPs, and FIDO Universal 2nd Factor (U2F) USB security keys.[44]

---

[42] PayPal adds authenticator app as 2-step verification option, ghacks.net, April 2019. Reproduced with permission from PayPal
How to enable 2FA for Pay, authy.

[43] NIST says push authentication is in, out-of-band SMS is out, Thales, August 2016

[44] See FIDO section of the white paper for explanation of U2F.

Increased Attack Surface

Many systems are involved in the delivery of an SMS or email, including internet protocols, wireless networks, email service providers that deliver OTPs, and other third parties that relay (e.g., SMS middleware, telephone companies, mobile operating system companies, voice-over-IP companies, internet service providers). Each has vulnerabilities. Finally, OTPs can be delivered to multiple devices (e.g., phone, computer, smartwatch, tablet) and accessed and read by multiple apps on each device. The more links in the chain, the more points of weakness there are to exploit.

Hijacked Phone Accounts

Phone accounts can be hijacked from a SIM[45] card. This occurs when a hacker with some knowledge of the victim (such as the last four digits of the Social Security number) calls the victim's phone carrier and asks to move the victim's phone number to the hacker's device to intercept the OTP. For example, a hacker used publicly available information to persuade AT&T to reassign a victim's phone number, then accessed the victim's PayPal account using SMS 2FA.[46]

Codes Sent in Plain Text

SMS and email messages are sent in plain text, which means that anyone who intercepts or get access to them can clearly read the OTP.

Unauthorized Viewing of OTPs

Many smartphone users enable text notifications to be visible on locked devices, so anyone could potentially read an SMS code by simply glancing over a user's shoulder without the user's knowledge.

2.3.6 Consumer Impact/Level of Friction

Consumer friction is minimal but depends on the type of OTP method. On-demand OTP delivery methods (delivered via email or mobile phone) generate the least friction. Consumers do not have to download and configure a separate app, as with soft token OTPs and push notifications; or carry a separate card, hardware token, or USB device,[47] as with many other authentication methods. On-demand delivery enables consumers to receive OTPs in real time, typically within a few seconds. Many people already have their email open on their mobile devices, and have easy access to their phone SMS messages, so accessing email and SMS OTPs is highly convenient.

2.3.7 Implementation Considerations

Multiple proprietary vendor solutions exist.

2.3.8 Maturity and Effectiveness of the Technique

OTPs add an important level of 2FA. While all the options/delivery methods have been available for many years, they vary in effectiveness as more payments are made digitally via mobile device.

---

[45] A subscriber identification module (SIM), widely known as a SIM card, is an integrated circuit that securely stores the international mobile subscriber identity (IMSI) number and its related key, both used to identify and authenticate subscribers on mobile phones and computers. SIM cards are always used on GSM phones; for CDMA phones, they are only needed for newer LTE-capable handsets.

[46] Security experts warn of account risks after Verizon customer data leak, Zdnet, July 2017

[47] Universal Serial Bus (USB) is a common interface that enables communication between devices and a host controller such as a personal computer (PC).

2.3.9 Applicable Industry Standards

- Internet Engineering Task Force (IETF)
- National Institute of Standards and Technology (NIST)

2.3.10 Publicly Available Statistics on Implementations and Use

Statistics are not available for this technique.

2.4 Mobile Public Key Infrastructure for Push-Based Authentication

2.4.1 Definition/Description

Push-based authentication (aka push notification authentication) validates login attempts by sending access requests via out-of-band notification to an associated mobile device. When the consumer registers an account, it is linked to their mobile device. When the consumer logs in to their account, they enter username or ID. Instead of entering a password, the consumer receives the push authentication request on their mobile device and is prompted to approve or decline the request with a tap. The server receives that request and proceeds with logging the user into the web or mobile application. While standard push notification services can deliver one-way messages, in mobile PKI systems the communication is encrypted bi-directionally (end-to-end) between the application and a secured authentication service.

A mobile application public key infrastructure (PKI) enables strong multi-factor authentication (MFA) for mobile transactions using industry standard cryptographic techniques to secure the authentication communication channel. Implemented primarily by issuing banks, this technique authenticates mobile transactions (in-app and browser) independent of the primary communication channel (e.g., https) through use of a mobile application. PKI provides a strong possession factor via issuance of a digital certificate that digitally binds the consumer to a trusted mobile device, which serves as an authenticator. It further allows for the creation and management of public and private key pairs, which are used to encrypt authentication messages end-to-end between the mobile device and a backend system (typically the card issuer). This allows the card issuer to reduce fraud and enables the consumer to be more involved in approving or denying transactions.

The system is characterized by using industry-standard strong encryption techniques and algorithms combined with digital signatures to provide online and offline authentication of transactions and onboarding into mobile wallets.

2.4.2 Applicability

The following payments scenarios are applicable with this technique:

- Authenticate mobile in-browser or in-app transactions
- Enable MFA to authenticate point-of-sale (POS) transactions (tap to pay)
- Authenticate provisioning of card to a mobile wallet (in the identity and verification process [ID&V])

Mobile PKI can be used to authenticate POS transactions and mobile in-app transactions, and provision cards to mobile wallets. It is typically combined with mobile push-based authentication to allow the consumer to authenticate in real time using multiple factors within a mobile application. Authentication can include capture of a knowledge (PIN, password) or inherence (facial biometrics, fingerprint) factor. These factors can then be validated either client-side (on the mobile device) or server-side (at the issuer) to complete the authentication. It is worth noting these authentication factors are in addition to the inherent possession factor provided by the digital certificate(s) issued to the consumer's mobile application or web browser.

2.4.3 Technical Features

Users need to be able to trust the authenticating device and trust that the key pairs are properly secured.

PKI is based on a series of trust relationships supported by applied cryptography and mathematics. To establish trust, a trusted authority (the certificate authority) issues digital certificates to a mobile device. The trusted authority issues a certificate to a consumer via a mobile application (typically that of the issuing bank) on behalf of the card issuer. These certificates should not be exportable or alterable, assuring the identity of the consumer is tied to the identity of their mobile device, which is used as a secure authenticator. Digital certificates contain specific identifying information, and their construction is governed by an international standard—X.509[48]. The certificates are combined with a public/private key pair that facilitates additional security features.

Furthermore, a mobile application on the device generates a private key, which it uses to encrypt and digitally sign transactions (authentication messages). This provides strong support for non-repudiation (i.e., protection against the consumer claiming they did not respond affirmative or negative to a particular authentication) for all transactions (e.g., mobile POS, mobile wallet provisioning, in-app purchases).

The key pairs are used to encrypt and decrypt authentication messages, providing for an end-to-end encrypted communication channel between the consumer's mobile device and the issuer's back-end systems. The public and private key pairs within the certificates encrypt, decrypt, and sign all authentication messages/transactions.

2.4.4 How the Technique Works

The following describes how the technique works.

- A mobile application generates a private and public key pair, analogous to the nearly universal TLS/SSL security used to secure web connections (e.g., browser sessions, application sessions).[49]
- A certificate authority issues a unique certificate to a device. This allows for passive single-factor authentication as the unique device ID serves as a strong possession factor. This is combined with push-based authentication, biometric validation, additional knowledge factor, and/or one-time-passcodes for strong MFA (using at least two of the three MFA factors following rules of inherence: what you know, what you have, who you are).
- The consumer's device is registered when the consumer registers with the issuer's mobile banking application.
- When the consumer initiates a mobile payment transaction or mobile wallet enrollment, the issuing bank uses PKI to send a push-authentication message to the consumer's mobile device via the mobile banking application.
- The signed authentication response is returned to the issuer for processing (e.g., transaction approval/decline).

[48] In cryptography, X.509 is an **International Telecommunication Union** (ITU) standard defining the format of public key certificates. X.509 certificates are used in many Internet protocols, including TLS/SSL, which is the basis for HTTPS, the secure protocol for browsing the web. X.509 - Wikipedia

[49] It is notable that PKI is the underlying technology that enables secure web communications and is the basis of the omnipresent TLS/SSL protocols (https).

2.4.5 Risks Associated with the Technique

The primary risk with this technique is improper implementation. The certificate-based nature requires that certificates be renewed (and rekeyed) periodically or the system will cease to function after the expiration date and time have been reached, jeopardizing the availability of the authentication tool. The system can resume functionality once the expired certificates are re-keyed but involves a higher level of effort than would have been incurred had the certificates been renewed/rekeyed before expiration.

Care must also be taken when registering the mobile PKI application to ensure that the mobile device serving as an authenticator belongs to the valid consumer. The mobile application should deploy additional security checks to ensure that the authenticating mobile device has not been compromised (e.g., malicious software has not been injected onto the device to capture or influence the authentication messages).

2.4.6 Consumer Impact/Level of Friction

When properly implemented, this technique minimizes consumer impact and enables "healthy" friction. Utilized in a mobile application, the consumer authentication experience becomes a simple proposition of selecting "yes" or "no" for a transaction and providing another factor if desired (e.g., biometric, PIN, password) for the push-based authentication.

Combined with a risk-based authentication (RBA) or rules engine, the user is only asked to authenticate during high-risk transactions, resulting in one of the simplest and most secure authentication mechanisms. This technique can be enabled for all transactions over a certain dollar amount, for example.

Unlike SMS OTPs, where a notification containing a code may be visible on a locked phone screen, push notifications do not contain a code, and the device must be unlocked to approve a notification. Even if a user's mobile phone is stolen, the device's PIN code or biometric protects against unauthorized access.

Also, notifications are sent in real time. If there is a fraudulent access request, the user can deny the request and act immediately, unlike reactive fraud alerts that only notify a victim after the fact.

2.4.7 Implementation Considerations

Mobile PKI requires a key management system (KMS), a certificate authority (CA), a decryption endpoint, and mobile application or applications that can interact with the decryption endpoints. These components are typically bundled together as part of a complete product package.

Mobile PKI, like most authentication tools, requires integration into an identity management system, so that transactions can be mapped to an identity and then correlated to the consumer's mobile device. Properly implemented solutions should also monitor the integrity and security of the authenticating mobile device to ensure there has been no malicious tampering.

Decisions need to be made for certificate handling, account provisioning, multiple device registrations, and other system functions before determining what solution to build or buy. Commercial vendor solutions are available.

2.4.8 Maturity and Effectiveness of the Technique

PKI-based authentication is highly mature and has existed since at least 1983, when RSA's security patent was published by the U.S. patent office.[50] The technique is the underlying mechanism for virtually all encrypted Internet-based communications and is utilized by billions of online users every day. The extrapolation of PKI to mobile devices has been in place since at least 2007 when BlackBerry incorporated the scheme into its mobile operating system.

This technique offers several advantages, including:

- High level of assurance if properly implemented
- Ease of use for the consumer
- Minimal maintenance
- Ability to work well with other authentication techniques

However, the technique may fall back to alternative authentication methods if the requisite mobile PKI-enabled application is not installed on the consumer's mobile device. The authenticating device must also be registered to the correct user (valid consumer).

2.4.9 Applicable Industry Standards

- NIST 800-63
- FIPS 140-2: Levels 1-3
- ANSI X9.31 (RSA algorithm)
- X.509 (cryptography standard)

2.4.10 Publicly Available Statistics on Implementations and Use

Statistics are not available for this technique.

[50] US Patent Office: Cryptographic communications system and method

2.5 Virtual Card Authentication

2.5.1 Definition/Description

Participating FIs[51] and some non-bank solutions[52] enable consumers (and small businesses)[53] to generate virtual card numbers to make online purchases in lieu of the real PAN with which it is associated. The cardholder creates a temporary or one-time-use card number, with security code and expiration date, linked to an existing card PAN.[54]

A variation is a virtual card number associated with a specific merchant that can be used for more than one purchase, but only with that specific merchant.[55]

Using a virtual card helps protect the consumer from becoming a victim of online fraud, however it should not be mistaken for tokenization.

2.5.2 Applicability

The virtual account works with credit cards for online or mobile-browser payments where a card number is typically entered. Virtual cards are not intended for payment at POS locations.[56] Stakeholders include issuers, merchants, processors, payment networks, and retail and small business consumers.

2.5.3 Technical Features

The issuer provides the virtual card feature through its online banking service. The consumer must have an existing online bank account and/or credit card with the participating issuer to enroll in the virtual card service. The consumer can request a virtual card number for a merchant, vendor, or other business. The issuer creates a unique card number that is stored for ongoing and future payments. Depending on the service, the consumer can indicate certain parameters (e.g., dollar limit and expiration date).

2.5.4 How the Technique Works

When the consumer wants to make an online purchase, they either log into their bank account to generate the virtual one-time number or request the virtual number while on the merchant website.[57] A card security code (associated with the virtual PAN) is also generated at that time. The consumer enters the virtual card number, expiration date, and card security code at the merchant's online checkout page, comparable to entering the real PAN.

---

[51] FIs include American Express (business only), Capital One (online only, not mobile) and Citi. Bank of America discontinued their 'ShopSafe' service in September 2019.

[52] Per Cardrates, Privacy and Entropay offer virtual card numbers.

[53] Corporate businesses may provide virtual cards to employees for travel, supply orders and other expense payments. These are out of scope for this authentication technique.

[54] Some FIs offer 'instant issuance' virtual cards with a very limited expiration period to enable customers to make purchases while waiting to receive their physical cards in the mail, but these are not considered 'virtual cards' for this white paper.

[55] "How to Get a Virtual Credit Card Number," Cardrates.com, February 2020. Some solution providers enable cardholders to set expiration dates and spend limits for each card and apply the same card controls and alerts provided for regular cards.

[56] Digital checkout wallets (e.g., Visa Checkout, Mastercard Masterpass) are not virtual credit cards.

[57] Varies by service provider.

Transactions made with a virtual card follow the same authorization process flow as the real PAN among the merchant/acquirer, payment network and issuer, but are more secure because the PAN can only be used once or associated with one specific merchant. After the authorization, the process is the same as a real PAN (e.g., liability, points, etc.).

2.5.5 Risks Associated with the Technique

The technique is primarily used as part of a layered approach to security, so risks associated with virtual cards is low. The consumer must login with username and password/passcode or biometric for authentication. Issuers and merchants should apply the same fraud analysis that they would use if they received a real PAN for the transaction. If the virtual card is single use, it limits the risk of fraud because it expires as soon as a purchase is made and cannot be reused if stolen.

Because the actual PAN is never revealed to the merchant, the virtual card cannot be traced back to the original PAN or to the consumer's identity.

For added control, consumers can set parameters, such as maximum credit limits (e.g., per transaction or per day), one-time use or specific retailer for an online purchase, or use during a specific time by setting an expiration date. If a fraudster copied the information to a physical card to use at POS, the card would be declined. Such parameters prevent the fraudster from successfully using the account number elsewhere. However, a fraudster that takes over an account could login as the legitimate cardholder and request a virtual credit card number for purchases.

Consumers enroll in the virtual card service through their issuer. The consumer authenticates each time they request a virtual card to make a purchase. However, a fraudster could enroll a stolen credit card in a bank's virtual card service and then use the bank's website to generate virtual card numbers.

2.5.6 Consumer Impact/Level of Friction

Virtual cards may introduce some friction for consumers, as noted below:

- There is potentially a higher decline rate due to factors such as attempted reuse, or short expiry dates.
- Virtual credit cards may not be accepted for purchases where the consumer must show the original credit card. For example, using virtual account numbers to rent a car or to purchase theater seats, which require the consumer's physical card at pickup, can be a challenge.

2.5.7 Implementation Considerations

Implementation efforts vary by issuer. Implementation requires software to enable consumers to request virtual card numbers, and an interface to the issuer's traditional card payment process. Issuers that do their own in-house processing may integrate with solution providers via cloud services, while payment processors may enable solution providers for real-time integration into their authorization streams.[58]

[58] CardHub, OnDot, Card Solutions, Digital Wallet | Fiserv, 2022

Issuers must determine if there is value in offering virtual credit card numbers as the industry moves to more comprehensive fraud alerts, digital wallets, and other secure payment solutions, which are becoming ubiquitous and are reducing the need for virtual card numbers. Most U.S. implementations today are for virtual commercial cards and accounts payable type products, including those for small business owners.[59]

2.5.8 Maturity and Effectiveness of the Technique

Virtual cards are very limited in use to fraudsters. Multi-use virtual card numbers cannot be used across merchants or vendors, and the dynamically created static card security code creates a number connected to the virtual PAN that cannot be reused by fraudsters.

Virtual credit cards can limit fraud risk of single-use virtual PANs because they are not stored anywhere that can be breached, so if stolen cannot be reused. Virtual cards replace the consumer's real credit card number, preventing compromise of the PAN. The virtual card is also relatively easy and convenient for consumers to obtain.

FIs and businesses have provided virtual account numbers for different use cases for over 10 years. Payment networks, PayPal and several large FIs have also offered them to their Visa, Mastercard or American Express (business) consumers. However, low usage and the development of more effective fraud tools (e.g., network tokenization[60] for digital wallets and card-on-file, artificial intelligence, and other risk management options) have limited the value of virtual account numbers, particularly for consumers. There is a niche market for small businesses to be able to make card payments more efficiently to their suppliers or other vendors.

2.5.9 Applicable Industry Standards

PCI compliance and other standards that apply to the use of traditional credit cards also apply to virtual cards.

2.5.10 Publicly Available Statistics on Implementations and Use

Statistics are not available for this technique.

[59] Single-Use Accounts, JPMorgan.

[60] Payment Tokens are surrogate values that replace the PAN as part of the payment process. EMVCo-Payment-Tokenisation-Specification-Technical-Framework-v2.2.pdf. They are provisioned by the card issuer to the cardholder and stored in the mobile device or cloud for NFC wallets depending on the provider, or in the cloud for digital wallets and CoF. Payment (network) tokens are used in lieu of the PAN when making mobile/digital-initiated purchases.

2.6 Consumer Device Cardholder Verification Method[61]

2.6.1 Definition/Description

The growing use of mobile devices for payment transactions has enabled consumer authentication to occur on the consumer's own device. The consumer enters a passcode, password, or pattern, or a biometric such as fingerprint, iris, voice or facial recognition on their mobile device. This type of authentication is known as Consumer Device Cardholder Verification Method (CDCVM) or On Device Cardholder Verification Method (ODCVM). CDCVM is primarily used in POS transactions; not everything will be relevant in the remote space.

2.6.2 Applicability

This technique applies to payment service providers and token service providers (TSPs), payment systems, mobile application providers and CDCVM solution developers, issuers, and merchants.

CDCVM is used to authenticate a consumer making a mobile-initiated card (credit, debit) payment transaction for both payment at the POS and for some CNP payments. Additionally, some biometric cards are being launched that allow for a card present, card-initiated transaction with CDCVM. The result of the authentication by the consumer device may be sent to the issuer.[62]

2.6.3 Technical Features

Cardholder credentials, including biometrics or passcodes, are stored and verified on the mobile device itself. Such verifications can occur even if the device is not connected to a mobile network.

The value to issuers and merchants includes:

- The issuer may get information about which CDCVM solution was performed.
- The merchant can get stronger cardholder verification for remote transactions.

2.6.4 How the Technique Works

The consumer must register to provision their chosen verification method in the wallet on the mobile device. Once the user has verified their payment credentials to the device, they can initiate a transaction.

The EMVCo Shared Platform Authentication diagram in Figure 2 shows how the authentication occurs through the shared platform.[63] The consumer biometric verification data is stored in the shared platform. During use, the consumer is prompted for the biometric data. Once the data is captured by the mobile phone, it is matched with the stored reference data and the result is sent to the mobile application requiring it.

[61] Mastercard uses the term ODCVM or 'On Device Cardholder Verification Method.'

[62] This does not apply to debit transactions via a domestic debit network.

[63] The process used for the verification of credentials and the indication of verification results can be shared between multiple mobile applications and wallets residing on the consumer device. This is known as 'shared CDCVM,' and helps to provide a consistent user experience if verification is needed for different uses, for example, payment, home banking or ticketing.

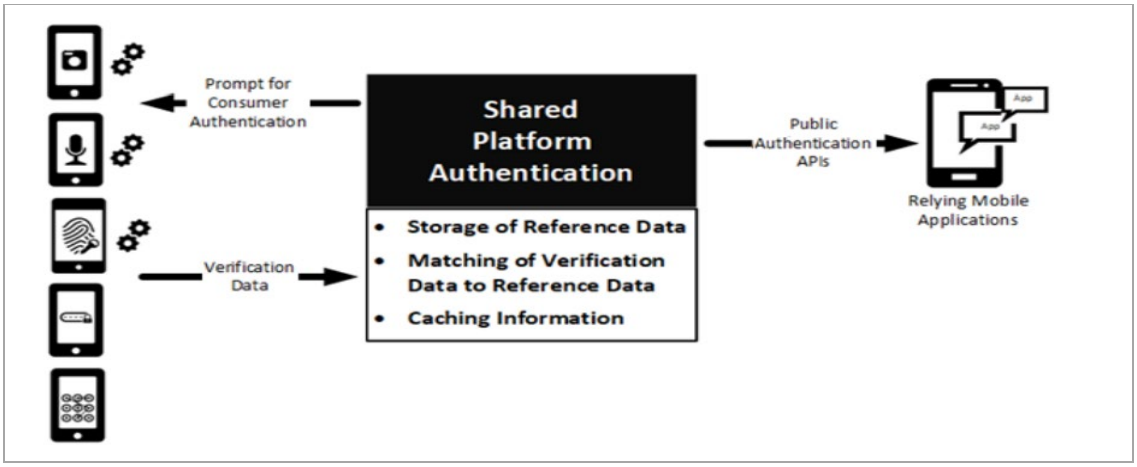

Figure 2. EMVCo Shared Platform Authentication[64]

2.6.5 Risks Associated with the Technique

Because CDCVM is generally a black-box solution, relative risks are unknown in the event a consumer device is stolen and the consumer has not taken steps to invalidate the assets on the device, or the device itself. For example, if a fingerprint scanner does not function effectively, it could result in many false positives. Additionally, CDCVM relies on a third-party vendor for implementation.

CDCVM introduces more complexity and variability than traditional CVMs, which can make it difficult for issuers to identify the exact CDCVM used for a particular payment transaction. CDCVM solutions can use varying components on a device, encompass multiple modalities, and be used across many consumer devices manufactured by different OEMs for various markets and users. To address this issue, EMVCo is creating a CDCVM solutions database that assigns each registered CDCVM solution a unique, short identifier known as an EMV CDCVM Solution ID.[65]

2.6.6 Consumer Impact/Level of Friction

This CDCVM solution uses device authentication to perform purchases and has minimal friction when biometrics is included.

2.6.7 Implementation Considerations

For CDCVM implementation practices and best practices, refer to the EMVCo publication, "Consumer Device Cardholder Verification Method—Best Practices."[66] The best practices focus on aspects of a CDCVM solution that are not covered in a solution security evaluation as defined by EMVCo.

2.6.8 Maturity and Effectiveness of the Technique

A number of solutions are available. For example, Apple Pay, Google Pay and Samsung Pay use CDCVM to verify the cardholder to the device and then perform the transaction, as do biometric card and wearable solutions.

---

[64] Consumer Device Cardholder Verification Method Security Requirements, EMVCo, September 2018
[65] CDCVM Solution ID, EMVCo, 2022
[66] Consumer Device Cardholder Verification Method—Best Practices, EMVCo, March 2019

Use of the consumer device to provide in-person verification to the relying applications[67] for purchase-related transactions includes multiple authentication mechanisms such as: passcodes (digits), passwords (alphanumeric characters), screen patterns, facial recognition, iris recognition, fingerprint, voice, and similar mechanisms that use the hardware provided by the device (e.g., screen, cameras, sensors, microphones). These are accessible to the consumer under a device settings menu to unlock a device and are generally shared and accessible to relying applications on the device through platform authenticator APIs.[68]

However, EMVCo has set security requirements including asset protection, solution protection, and verification result, among others, that the solutions must provide to block/reduce fraudulent access to the solution. In addition, for software-based mobile payment (SBMP) devices, the EMVCo Security Evaluation Process assesses whether a component or solution demonstrates sufficient assurance of certain minimum levels of security, including security mechanisms and protections designed to withstand known attacks.

2.6.9 Applicable Industry Standards

- EMVCo Publication, "Consumer Device Cardholder Verification Method Security Requirements" Version 1.0, September 2018
- EMVCo Publication, "Consumer Device Cardholder Verification Method—Best Practices" Version 1.0, 15 March 2019

2.6.10 Publicly Available Statistics on Implementations and Use

Most modern mobile phones based on iOS and Android operating systems support CDCVM.

[67] Relying party/mobile application applies to the mobile application that uses a CDCVM solution to provide consumer authentication functionality. Consumer Device Cardholder Verification Method—Best Practices, EMVCo, March 2019

[68] Consumer Device Cardholder Verification Method Security Requirements, EMVCo, September 2018

2.7 EMV Secure Remote Commerce (SRC)

2.7.1 Definition/Description

Secure Remote Commerce (SRC) is a specification created by EMVCo and first published (version 1.0) in June 2019. EMVCo created SRC to:

- Promote secure, consistent, and interoperable card acceptance in CNP transactions established through a technical framework and specification.
- Enable a merchant to securely request and receive interoperable payment data during checkout to process a payment for a remote commerce transaction.
- Create consumer convenience by minimizing the entry of payment credentials at every merchant.
- Introduce a framework to result in reduced fraud, false declines rates, and shopping cart abandonment due to checkout friction.
- Leverage existing authentication and fraud reduction systems, such as payment tokenization and EMV 3-D Secure, to share data and make better risk decisioning.

The specification outlines the relevant participants and roles, APIs, system requirements, assurance methods, and data payloads. At its core, SRC is focused on consumer authentication as distinct from cardholder authentication, although it should be noted that cardholder verification methods may be invoked during SRC provisioning. This allows SRC to serve as a framework that allows authentication data—from any potential source—to be securely and uniformly shared among all participants.

To simplify the user experience in online commerce, the payment networks have transitioned from individual "one click" payment options (e.g., Mastercard Masterpass, Visa Checkout) to a new model, SRC. The EMVCo SRC specification was created to bring consistency to the integration, process, and consumer experience of "click to pay" checkout services. The specification covers the process for secure exchange of payment data, the use of tokens/cryptograms as replacements for PANs during checkout, and integration with other technologies and standards, such as EMV 3-D Secure.

With SRC-compliant checkout services, users enroll their payment information with the service through their merchant or their card issuer, which then facilitates data transmission between the merchant, issuer, and other parties in the payment process. Merchants have the option to replace the user's card number with a token to eliminate the need to transmit or store the PAN.

To make a purchase, the consumer clicks on the checkout icon. If they are using a new device, they may be required to authenticate to the payment service. If tokenization has been added, the tokenized payment information is transmitted to the merchant.

2.7.2 Applicability

SRC applies to all remote card-based transactions (other payment methods are out of scope for SRC). These transactions can be consumer-initiated, where the consumer actively activates an SRC trigger (e.g., at checkout), or a merchant-initiated transaction (such as a recurring payment). SRC supports multiple transaction types, including in-app, in-browser, and IoT.

2.7.3 Technical Features

SRC relies on a network of SRC participants to coordinate and communicate dynamic data. The SRC participants are defined as follows:

- Digital Payment Application (DPA). The DPA enables the checkout experience used for the interaction of a consumer with a merchant. Most typically, the DPA will be part of a checkout initiated after the consumer has selected goods or services and is in the process of paying. The checkout can also be merchant-initiated (e.g., for a recurring payment).
- SRC Initiator (SRCI). The SRCI aggregates multiple SRC systems to bring the information back to a single user interface and acts as the middle layer between the merchant and SRC systems. SRCI performs card presentment assessed from DCF and SRC system availability and populates the list of available cards in a particular SRC System. Once a consumer selects a card, they are "transferred" to the associated DCF. An SRCI example would be a third-party payment service provider (PSP).
- Digital Card Facilitator (DCF). The DCF provides the interface to access digital cards within the SRC systems (note that SRCI is the aggregator). The DCF is where the consumer verifies identity, potentially through existing cardholder authentication methods, has access to shipping and delivery information, and can validate the information. The DCF facilitates the delivery of PAN-related data to the SRC system. Additional cardholder authentication may be performed in the DCF. The DCF is generally analogous to a digital wallet.
- SRC System (i.e., the payment network). The SRC System serves as the "orchestration layer," managing all the activities among the various participants and systems and maintaining the interactions among them. It stores the SRC profiles for retrieval by the SRCI and facilitates the secure exchange of payment information across the systems.
- SRC Participating Issuer (SRC PI). The SRC PI is the participating bank that issues the consumer payment card(s). The SRC PI may have their payment cards in one or multiple DCFs (e.g., "wallets") and must have a relationship with one or more card schemes. The SRC PI is also responsible for SRC token lifecycle management including creation, renewal, and revocation.

Additionally, although not a participant role, the SRC profile is a critical component because it correlates PANs, DCFs, consumer IDs, device IDs, and other data elements, allowing for orchestration within SRC. The SRC profile is stored inside of its respective SRC System. As such, there can be multiple SRC profiles associated with a consumer, depending on the number of SRC Systems that the consumer is enrolled in.

An SRC JavaScript SDK is also available to enable rapid adoption of the technology. The SDK provides a standard SRC checkout experience and view that can be deployed at any participating merchant (or DPA).

2.7.4 How the Technique Works

To use SRC, a consumer must have an SRC-eligible payment card, determined by the SRC PI. Once the SRC PI has established eligibility, the DCF will facilitate binding the consumer device for recognition during subsequent checkouts, using a variety of authentication methods (described in other sections of this white paper). Enrollment in the DCF allows the consumer to enter their payment card credentials only once in the chosen DCF and eliminates the need for credentials to be re-entered going forward.

A merchant (i.e., DPA) will initiate an SRC checkout or a merchant checkout, either as a cardholder-initiated or merchant-initiated checkout. Once the checkout is initiated, the SRCI will interrogate the SRC System to discover if the consumer has an SRC profile that matches and is in the available SRC systems. If a match is found, the SRCI aggregates the available cards and associated DCFs for card selection. Once the card is selected, the associated DCF is invoked to handle presentment of card details and consumer details (e.g., shipping and delivery information) and perform additional authentication if needed (e.g., step-up). After the DCF completes the checkout and card selection, all the requested data is returned to the merchant—including either a PAN or tokenized PAN—for submission to the payment service provider.

2.7.5 Standalone vs. Layered Approach

SRC is, by definition, a layered approach as it orchestrates multiple participant data sources and aggregates authentication and assurance data during a CNP checkout. SRC uses consumer, cardholder, card, and device authentication as well as binding, encompassing a variety of implicit authentication techniques.

2.7.6 Risks Associated with the Technique

Primary risks are onboarding a bad actor, familial fraud (e.g., family members having access to the trusted DCF device), or a replay attack (e.g., device spoofing/cloning issues).

As SRC is a relatively new framework, the successful adoption of SRC has yet to be determined. Details and any potential risks are still unclear, and best practices are still being determined. As time goes on, most associated risks should be identified and addressed. However, SRC systems combine dynamic and encrypted data to help reduce risk of fraud. Payment card information is stored with the SRC System, and may be tokenized, which reduces the need for the merchant to store PANs

2.7.7 Consumer Impact/Level of Friction

SRC aims to create a more secure and consistent consumer checkout experience across digital channels that reduces overall consumer friction. By leveraging a federation of securely stored card details in the DCF and SRC System, SRC eliminates the need for consumers to enter payment card details during checkout.

The ability to increase authorization rates, receive additional data, and reduce fraud may encourage issuers to adopt SRC. However, issuers must consider the risk of auto-enrollment.

2.7.8 Implementation Considerations

As a new technical framework, best practices will evolve as SRC gains adoption. The core principles of the systems that must be implemented are outlined in the EMVCo specification.

2.7.9 Maturity and Effectiveness of Tool

An advantage of SRC is the shared authentication and assurance data among SRC participants, giving the merchant more data to help make decisions, while simultaneously reducing fraud and providing a superior consumer checkout experience for CNP. SRC can also be utilized in non-traditional CNP checkouts such as IoT.

Since the EMV SRC specification was published in 2019, EMVCo continues to evolve the specification in response to changing industry requirements, monitoring the industry and implementations to understand areas to be enhanced, improved, and maintained.

2.7.10 Applicable Industry Standards

- EMV Secure Remote Commerce Specifications v1.0[69]

2.7.11 Publicly Available Statistics on Implementations and Use

Statistics are not available for this technique. SRC is a relatively new framework and has not yet been fully implemented.

[69] Secure Remote Commerce - EMVCo, June 2021

2.8 Biometrics

Biometrics used to digitally identify a person fall along two continuums: active vs. passive, and physical vs. behavioral. Active biometrics are those which require a person to take an overt action, such as placing finger on a reader. Passive biometrics are measured in the background using an interaction that is part of the overall transaction, such as a keystroke. Physical, or biological, biometrics detect some part of the body such as facial recognition. Behavioral biometrics instead detect an action or activity such as touchscreen interaction.

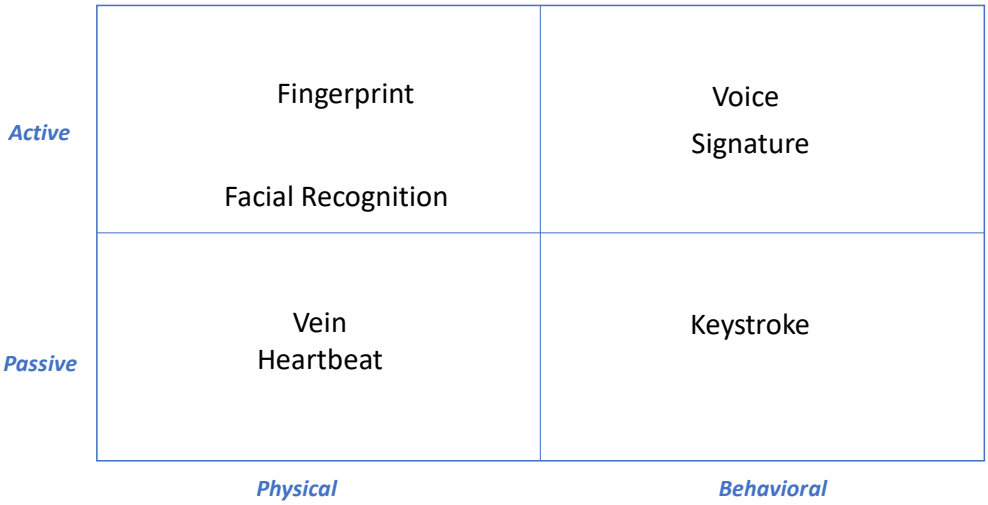

Figure 3. Physical vs Behavioral Biometrics, Active vs Passive

2.8.1 Physical Biometrics

2.8.1.1 Definition/Description

Just ten years ago, biometrics were the stuff of science fiction, but today we think nothing of inputting our fingerprints to unlock our phones. Active physical (fingerprint and facial recognition) and behavioral (voice and signature) biometrics require user participation and compliance. This includes pre-registering, or enrolling, the biometric via fingerprint, face or iris scanning, or voice recording.

2.8.1.2 Applicability

Physical biometrics apply to mobile app login, payment transactions, step-up authentication, re-enrollment, and device binding.

2.8.1.3 Technical Features

Depending on the biometric modality used, this technique might require special hardware (e.g., camera or sensors) to capture the specific features or series of samples. Processing and comparing the features takes place through dedicated algorithms that maintain the accuracy and speed required for each use case.

2.8.1.4 How Technique Works

Capturing and processing each user sample pattern is different depending on the model, as outlined in Table 1.

Table 1: Biometric Models

MODEL	PROCESS	EXAMPLE CHALLENGES
Fingerprint	Capturing and matching minutiae and patterns	Does not work well with some populations (e.g., dry skin)
Face	Using spatial geometry comparison	Interference with cosmetics, shaving, hats, glasses, or masks might challenge the accuracy and success rate
Voice	Digitizing the user speech and producing a unique model	Could be text dependent (e.g., using passphrase of 2-3 words) or text independent
Iris	Using statistical independence, which involves degrees-of-freedom or analyzable features	Quality of image captured

2.8.1.5 Risks Associated with Technique

According to a 2019 NuData report,[70] the following are vulnerabilities associated with physical biometrics:

- Not always socially or culturally appropriate; can be awkward in some situations
- Consumer friction, especially if consumer is repeatedly challenged
- Subject to theft, during capture, storage, or physically from objects (e.g., fingerprints, high-definition photos)
- Privacy and consent issues
- Need to ensure the liveness (e.g., warmth in finger, movement)
- Force in cases of abduction or amputation
- Changing nature of some biometric (e.g., blood-vessel patterns, thinning of skin, cut on fingers)

Consumers should be aware that a physical biometric is not a foolproof marker of one's identity. Biometric data can be vulnerable to mimicry, spoofing and impersonation. Fingerprints can be lifted, spoofed, and copied. There is still no absolute certainty that the presenter of the biometric is the owner.

Most importantly, biometrics are permanent. The mostly unchangeable nature of biometrics presents a permanent lifetime consumer risk if biometric data is stolen. Consumers are dependent on the vendor or provider to adequately protect their data; therefore, great care must be taken with any biometric storage, and the mere storage of this data can make organizations attractive targets.

2.8.1.6 Consumer Impact/Level of Friction

Since this technique is visible to users, it could cause friction especially if certain accuracy is required. The right balance between security risk, which might lead to fraud in the future, and more friction which might increase the user abandonment rate, must be assessed closely.

[70] The Next Evolution of Authentication, NuData, 2019

2.8.1.7 Implementation Considerations

Proper implementation should consider enrollment threats – e.g., an illegitimate user enrolling someone else's credentials. Local storage and comparison are preferred for the sake of security and integrity. It is also preferable to include liveness detection to detect potential attacks.

2.8.1.8 Maturity and Effectiveness of Tool

There are many companies that offer physical biometric solutions. The technique is relatively mature in the mobile payment space, deployed by nearly all modern smart phones for authentication.

2.8.1.9 Applicable Industry Standards

- NIST: involved in many biometric standards developments, including those at the Federal government level
- ISO/IEC Joint Technical Committee 1, Subcommittee 37- Biometrics
- Homeland Security Presidential Directive (HSPD)-12/FIPS 201
- American Association of Motor Vehicle Administrators (AAMVA): ID barcode and other data fields in IDs and driver licenses
- International Civil Aviation Organization (ICAO): defines the passport document standards

2.8.1.10 Publicly Available Statistics on Implementations

Jupiter forecasts that 95% of smartphone will be biometric enabled for authentication by 2025, up from 41% in 2020. Although fingerprint readers remain the top option for authentication, voice and facial recognition are catching up: voice usage doubling to 20% and facial recognition tripling to 30% in 2020.[71]

2.8.1.11 Use Case: ID Document Scan

This use case uses the mobile device camera to capture the ID document and send the captured image for processing in which data will be extracted (e.g., name, birthdate, and address) and security features automatically checked. This is done via advanced image processing and machine learning techniques to classify, run security checks and provide a verdict in real time.

Using ID scan, consumers can remotely verify their identity and save time filling in forms with personal details that can be captured automatically from the ID document, resulting in better data quality and faster enrollment process.

Liveness detection involves capturing a short video stream of the consumer face (e.g., via the front selfie camera) and validating some facial expressions or other liveness detection features. The captured images are compared against the consumer photo in the ID to complete the full authentication cycle. See Figure 4.

[71] Billions of Smartphone Owners Will Soon Be Authorizing Payments Using Facial Recognition, ZDNet, 2021; By 2024, How Many Smartphone Owners Will Use Biometrics?, Payments Journal, June 2020

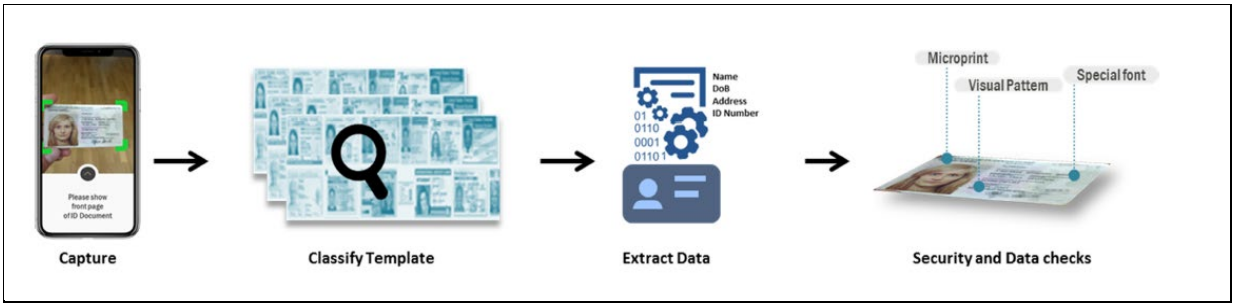

Figure 4. ID Scan Process[72]

This technique is a ready solution with a long list of live deployments available today in the marketplace. Some regulations might require further geographical limitation or other security practices to be implemented.

2.8.2 Behavioral Biometrics

2.8.2.1 Definition/Description

Along with device information, behavioral biometric solutions measure uniquely identifying patterns in human activities, including keystroke dynamics, gait analysis, voice ID, mouse use characteristics, signature analysis and cognitive biometrics.[73]

Behavioral biometrics are distinct from "biological" biometrics in that "behavioral" implies an activity of some sort, such as signing one's name, talking, typing, using a touch screen, or walking. When sufficient behavioral information is collected, the system can confirm that the user of the system is the same as the user on record. It can also detect if the user is a different user or a bot, or flag suspicious behavior that might indicate account opening fraud, in which case there is no original genuine user to compare to. Behavioral biometrics can establish a risk rating associated with each transaction that reflects a finely calibrated level of confidence that the user is not only a person, but the right person.

The interest in behavioral biometrics is in part driven by new European banking rules, increase in machine learning and the drive to replace passwords.[74]

Behavioral biometrics started with relatively straightforward authentication of a user to be genuine, based on comparing behavioral attributes with an established, trained model of the real user. The use of behavioral biometrics evolved over time to detect new kinds of fraud use cases, including:

- **Account takeover**: new attributes such as device reputation, bots, remote access tools and malware, and new patterns indicating likelihood of criminal user. These new patterns of behavior reflect extreme familiarity with the web site's processes, and unfamiliarity with the data, exactly the opposite of a genuine user. Examples include pasting names, use of arrow keys instead of the mouse, no hesitancy in entering unusual data that a genuine user would have to spend some time to search for, or not using autofill.
- **Account opening using stolen PII:** new techniques and attributes similar to account takeover, with the added complication that there is no genuine user for comparison.

[72] Mina Malek, Giesecke & Devrient, June 2019
[73] Whatis.com
[74] What's Behind the Rise of Behavioral Biometrics?, PYMNTS.COM, August 2018

- **Deep social engineering**: subtle behavioral changes such as indicating hesitancy or being dictated to. In this case, the genuine user is conducting the transaction, but they are being tricked by a criminal. If detected, the bank may choose to call the user to confirm the scenario: "did somebody call you and ask you to do this?"

2.8.2.2 Applicability

Behavioral biometrics technology is applicable to mobile browser and in-app, and has been deployed in four types of applications:[75]

1. Continuous authentication. Since behavioral biometrics are completely passive, they enable continuous authentication.
2. Risk-based authentication. Behavioral biometrics can be used to augment other data such as device type, IP address, geolocation, and historical behavior.
3. Insider threat detection. Behavioral biometrics lessen the risk of employees exploiting knowledge of security practices.
4. Fraud detection and prevention. Behavioral biometrics can be imbedded into fraud detection tools to root out bots and other threats.

2.8.2.3 Technical Features

Behavioral biometrics must be fine-tuned to continuously discover non-human device activity, such as those caused by bots, malware, remote access trojans (RATs), automated scripts and fraud-focused emulators.

2.8.2.4 How the Technique Works

With behavioral biometrics, a biometric sample is captured. The biometric sample is converted into a template and compared to a template in the database. The matching algorithm issues a score indicating the probability that both samples belong to the same person. A decision module approves the authentication based on the score. See Figure 5.

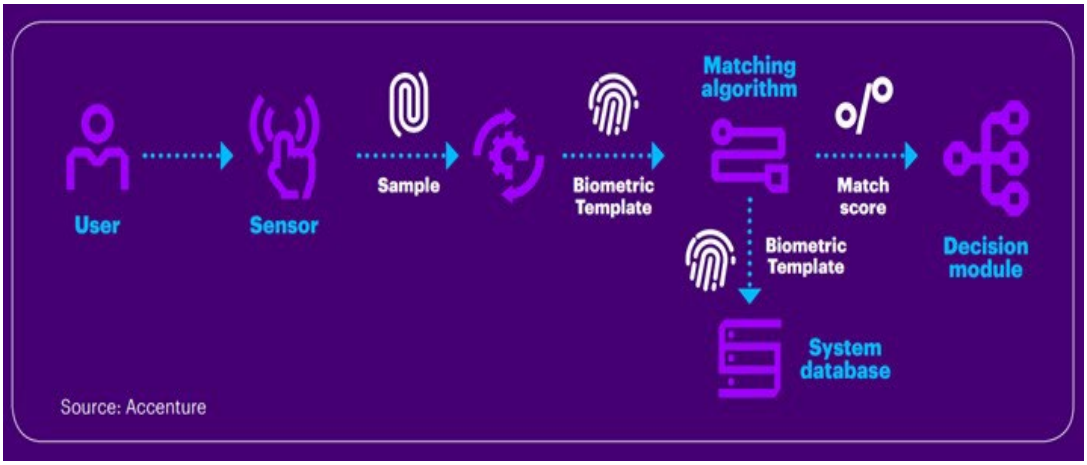

Figure 5. Matching Process[76]

[75] Behavioral Biometrics, International Biometrics+Identity Association, May 2017
[76] Biometrics Applied to Payments, Accenture, 2018

The accuracy is measured by two ratios, which intersect at the Equal Error Rate:

1. False Accept Ratio (FAR) is the percentage of samples incorrectly scored above the threshold. The higher the threshold, the less likely that incorrect samples are accepted.
2. False Reject Ratio (FRR) is the percentage of samples incorrectly scored below the threshold. The lower the threshold, the less likely that correct samples are rejected.
3. Equal Error Rate (ERR) is the threshold at which FAR and FRR intersect. ERR is generally used to determine the accuracy of a system.

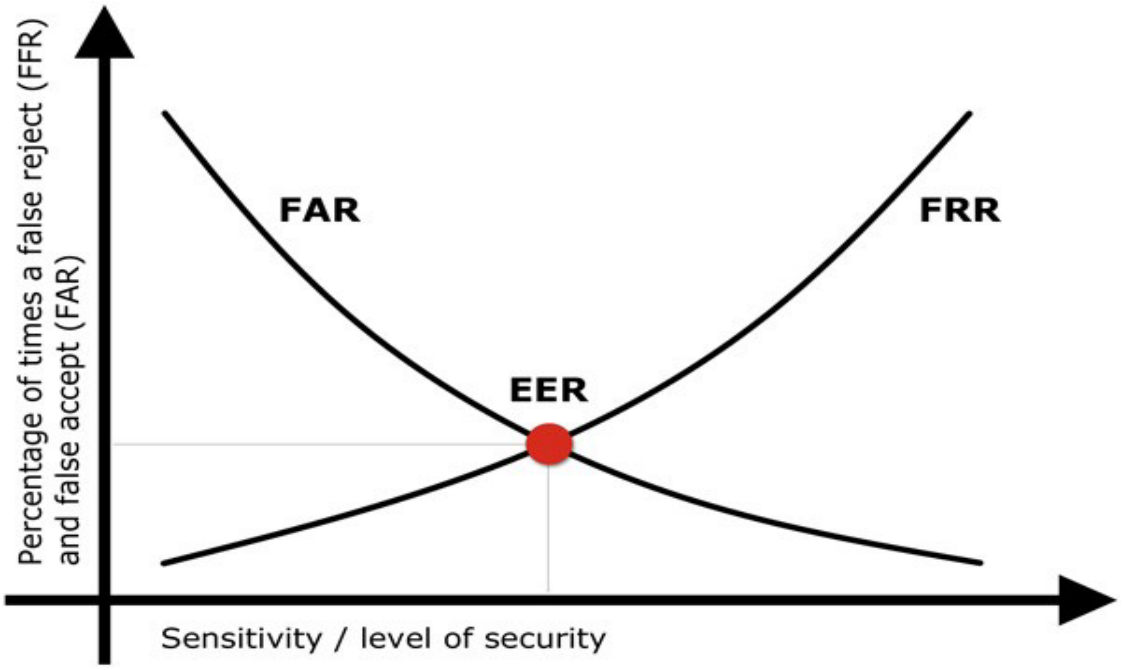

Figure 6. FRR and FAR Curve Matching Point[77]

2.8.2.5 Risks Associated with the Technique

While consumers will enjoy a more seamless experience, the industry must exercise extreme caution since biometric data can't be changed – once compromised the impact on consumers could be catastrophic.[78] However, a case can be made that behavioral biometrics are more privacy friendly since the data points cannot be used to identify a person. Behavioral biometrics are agnostic with respect to PII.[79]

Behavioral biometrics are less stable than biological traits and can change over time, leading to the need for continuous refreshment of reference data.[80]

2.8.2.6 Consumer Impact/Level of Friction

Since enrollment is in the background during the transaction process, behavioral biometrics are completely frictionless[81] and can reduce the need for step-up authentication.

---

[77] FAR and FRR: security level versus user convenience, recogtech

[78] Behavioral biometrics and biometrics in payment cards: Beyond the PIN and password, Gemalto, February 2020

[79] Behavioral Biometrics, International Biometrics+Identity Association, May 2017

[80] Gartner Technology Insight for Biometric Authentication, November 2018

[81] Behavioral Biometrics, International Biometrics+Identity Association, May 2017

2.8.2.7 Implementation Considerations

Typically, 10 interactions are needed to establish a baseline for passive biometrics; these modes are most reliable when a consumer interacts on a regular basis (e.g., a few times a month).[82] However, as discussed earlier regarding the evolution of tools to detect new kinds of fraud including account opening fraud, account takeover and deep social engineering, continuous diligence is required to detect the ever-evolving face of new fraud types. This may require the addition of new attributes and retraining of models.

2.8.2.8 Maturity and Effectiveness of Tool

BehavioSec claims to correctly identify consumers 99.7% of the time, while also detecting an imposter 99.7% of the time, a very high level of accuracy among all types of biometrics.[83] BioCatch claims over 90% accuracy rate on new account fraud alerts.[84]

2.8.2.9 Applicable Industry Standards

- ANSI X9.84-2018: Biometric Information Management and Security for the Financial Services Industry
- International Biometrics Identity Association (IBIA.org) advances the adoption and responsible use of technologies for managing human identity to enhance security, privacy, productivity, and convenience for individuals, organizations, and governments.

2.8.2.10 Publicly Available Statistics on Implementations and Use

Statistics are not available for this technique.

[82] Gartner Technology Insight for Biometric Authentication, November 2018
[83] BehavioSec in a Real World eBanking Environment, Behaviosec, October 2018
[84] New Account Opening Fraud: 3 Ways Behavioral Biometrics Can Spot Criminals and Protect Customers, BioCatch, 2020

2.9 FIDO (Fast Identity Online)

2.9.1 Definition/Description

FIDO is an acronym for Fast Identity Online, freely available open technical standards created by the FIDO Alliance that utilize on-device public key cryptography to authenticate a user to an online service. The FIDO Alliance aims to replace traditional on-server password authentication with a possession-based public-private key pair similar to that used by EMV card chips. To date, FIDO has published three sets of standards for authentication:

- **FIDO Universal Authentication Framework** (FIDO UAF) is an open protocol designed to offer passwordless MFA for online services, typically utilizing on-device biometrics such as fingerprint and facial recognition. FIDO UAF is primarily deployed on mobile devices.
- **FIDO Universal Second Factor** (FIDO U2F) is a standard designed to utilize certified USB, Near Field Communication (NFC) and/or Bluetooth security keys to provide a second strong authentication factor.
- **FIDO2** is a set of technologies that enable passwordless authentication between servers, browsers, and authenticators. It is the most recently published standard developed jointly between the FIDO Alliance and the World Wide Web Consortium (W3C) to broaden FIDO authenticator acceptance on web browsers and operating systems. FIDO2 standards enable users to leverage common devices to easily authenticate to online services in both mobile and desktop environments, with much higher security over passwords and SMS OTPs.

  FIDO2 is comprised of the W3C WebAuthn specification and corresponding Client-to-Authenticator Protocols (CTAP) from the FIDO Alliance. FIDO2 supports passwordless, second-factor, and multi-factor user experiences with embedded (or bound) authenticators (such as biometrics or PINs) or external (or roaming) authenticators (such as FIDO Security Keys, mobile devices, wearables). Many FIDO UAF and FIDO U2F deployments are in the market globally. With the release of FIDO2, FIDO U2F capabilities have merged into the FIDO2 CTAP protocol, and FIDO U2F has been renamed CTAP1. As a result, most new deployers of FIDO authentication will choose FIDO2 and/or FIDO UAF specifications, depending on their use case.

2.9.2 Applicability

FIDO authenticates users to any online service, including online banking and ecommerce apps and websites. FIDO can also be used for step-up authentication or payment authorization within banking and ecommerce apps and websites. FIDO Certified authenticators on mobile devices, PCs and FIDO Security Keys are increasingly available in the consumer market. (For example, any Android 7 or later and any Windows 10 PC are FIDO Certified.) They can be leveraged for user authentication and/or remote payment transactions if the bank or ecommerce merchant has enabled support for the FIDO technology and the user has registered an authenticator.

2.9.3 Technical Features

FIDO uses public key cryptography to provide challenge-response authentication and remove the need for a user to utilize an on-server credential such as a password. FIDO uses public-private key pairs where the private keys are generated on the FIDO authenticator device and never leave the device, ensuring the key cannot be easily exfiltrated. This allows for the digital signing of transactions with a user's key and increases the overall security of an authentication session.

2.9.4 How the Technique Works

When a transaction requires authentication, there are two steps for FIDO authentication:

1. A gesture between the user and the authenticator verifies that the user is present. The type of interaction required varies, but all require the FIDO authenticator to have been registered to a service to function. The authenticator verifies the gesture directly.
2. The authenticator authenticates the user to the service using public key cryptography.

Typically, the user authentication experience or transaction authorization once a user is registered is as follows:

- **FIDO2**. A user performs a gesture (e.g., swipe a finger, look at a camera and/or press button) on a FIDO-capable device (e.g., mobile phone, laptop fingerprint reader, FIDO Security Key) to prove possession. FIDO2 can be deployed as a passwordless or multi-factor experience.
- **FIDO U2F** (capabilities now part of FIDO2). A user presents a physical USB, NFC and/or Bluetooth security key to prove possession of the FIDO authenticator (possession factor) in addition to the password. A second interaction must be completed, such as tapping a button on the FIDO authenticator. This prevents a user whose FIDO authenticator is connected to a system from accidentally authenticating a session by virtue of having the authenticator inserted alone (i.e., plugged in).
- **FIDO UAF**. The user no longer needs to enter a password when authenticating from the registered mobile device. The user instead selects a local authentication mechanism, such as swiping a finger, looking at the camera, speaking into the microphone or entering a PIN.

FIDO works in concert with strong enrollment and account recovery procedures. The requirement for the FIDO authenticator to be enrolled in a particular service necessitates additional systems in order validate a user prior to enrollment. There should also be fallback mechanisms available to authenticate a user if the FIDO authenticator is lost, stolen, or otherwise unavailable.

2.9.5 Risks Associated with the Technique

The principal risk for FIDO authentication is in the enrollment process. Because all FIDO authenticators must be enrolled and associated to a user, it is possible that a bad actor with sufficient credentials (e.g., userID and password previously stolen) and access could maliciously enroll their own FIDO authenticator. In this scenario, the bad actor would then be able to masquerade as the legitimate user and perform authentications unencumbered.

2.9.6 Consumer Impact/Level of Friction

As FIDO is designed to be both a primary and secondary authentication factor, some consumer friction is necessarily involved. All FIDO authenticators must be enrolled into each individual service or application for which FIDO authentication is desired, creating friction before the technique can be utilized.

The subsequent level of friction depends on the type of FIDO authenticator used.[85] The use of security keys (supported in FIDO U2F and FIDO2) is commonly seen as generating a higher level of friction because a physical device must be inserted into a computer and a physical action performed to complete the authentication. FIDO authentication methods leveraging authenticators built into the various devices that are common in the consumer market (supported in FIDO UAF and FIDO2, such as fingerprint readers on mobile devices and laptop computers) generally provide lower levels of friction. However, any friction encountered might be viewed positively in that the consumer knows that they are proactively protecting their accounts.

Lastly, if a FIDO authenticator is lost or stolen, a user must re-enroll to any/all services for which they want to utilize FIDO. If there is no self-service option to re-enroll the user, contacting a service or call center may be necessary to validate the user's identity and allow for re-enrollment of a new FIDO authenticator.

2.9.7 Implementation Considerations

The specifics for implementation depend on which FIDO standard is being utilized. There are, however, central implementation concepts that apply for all three standards as shown in Figure 7 and Figure 8:

- A relying party: the service or application against which the user is trying to authenticate (e.g., a mobile payment application). The relying party can be thought of as a back-end system – for example, the bank hosting the online banking site or a mobile app.
- FIDO client: software on the user's device that handles the interaction between the FIDO server and the FIDO authenticator.
- FIDO server: server providing the ability for a relying party to perform FIDO authentication. It maintains login policies, management of public keys, and verification of the signatures created.
- FIDO authenticator: a device that is integral either to the device that is being utilized during the time of an authentication request or to an external device that is being leveraged in tandem with the current authentication session.

[85] User experiences cannot be divided by specification, as FIDO2 supports previous FIDO U2F scenarios as well the scenarios mentioned here.

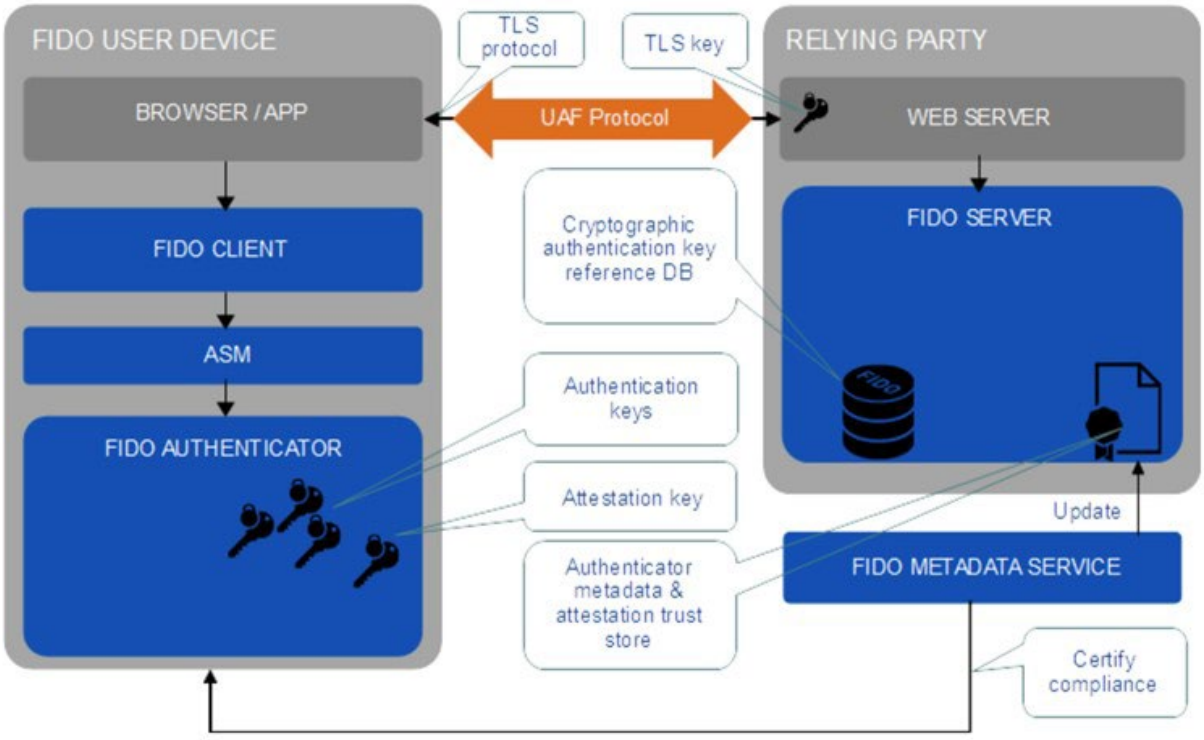

Figure 7. High-Level UAF Diagram[86]

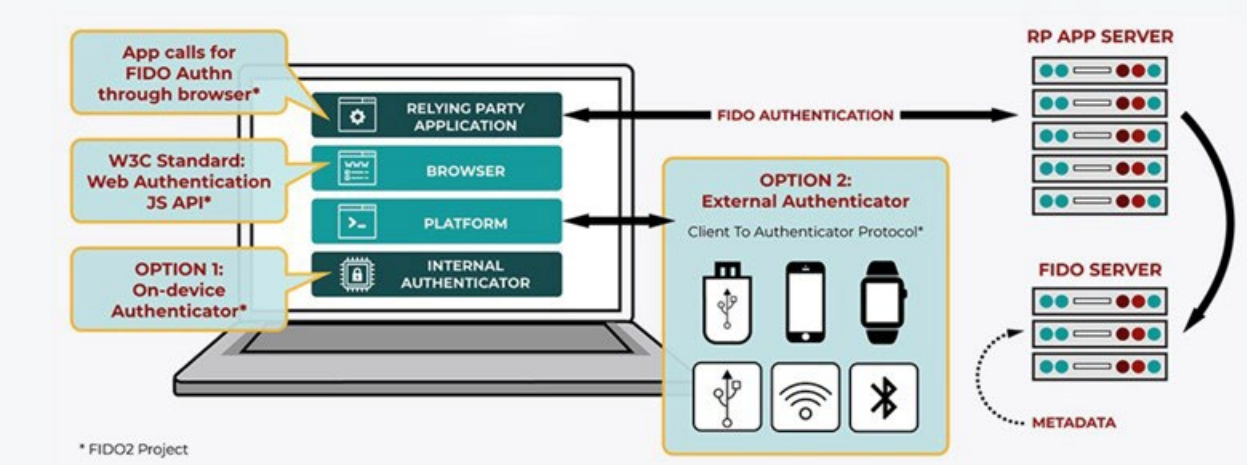

Figure 8. High Level FIDO2 Architecture (includes FIDO U2F now CTAP1)[87]

[86] FIDO UAF Architectural Overview, FIDO Alliance, February 2017

[87] FIDO2: WebAuthn & CTAP, FIDO Alliance

2.9.8 Maturity and Effectiveness of the Technique

The FIDO Alliance was founded in 2012 and publicly launched in February 2013, with the first UAF and U2F specifications completed in 2013.[88] FIDO has since published revisions to the initial UAF and U2F specifications, as well as creating the new FIDO2 specifications.

Support for FIDO authentication is broadly available in consumer devices, including mobile devices. Since February 2019, Android devices natively support FIDO APIs. Mobile versions of Apple Safari also support FIDO from iOS version 14 onward.

FIDO implementation provides several advantages.

- FIDO authentication removes the need to transmit any knowledge factors (e.g., password), which greatly reduces a bad actor's ability to intercept and replay said factors. The challenge-response and biometric capabilities require a bad actor to physically steal a user's authenticator. The inherent security is provided with public-private key pairs. Also, such attacks are not scalable, reducing the threat of credential stuffing or phishing.
- No sensitive information is stored in the cloud. If a data breach occurs, no sensitive data can be stolen. All sensitive information is stored on the device itself.
- All major browsers and platforms have implemented support for FIDO.
- FIDO authentication is interoperable with EMV 3DS.
- FIDO2 has multiple implementation options available to address a variety of use cases across multiple form factors (e.g., mobile phone, laptop). Service providers have many FIDO Certified solutions to choose from, or they can roll out their own implementations. FIDO2 provides deployment flexibility and interoperability.

Challenges with FIDO implementation include the following:

- Consumer challenges. Consumer friction can be high if enrolling into multiple services and applications. If the FIDO authenticator is lost or stolen, the user may be temporarily locked out of services that require that FIDO authenticator. The user will also need to re-enroll a new FIDO authenticator if desired. Most internet-connected consumer devices (e.g., laptops, mobile phones) ship with built-in security capabilities and on-device biometric authenticators to support FIDO. However, the evolution of consumer awareness and relying party willingness to show FIDO branding are still in the early stages and are needed to build adoption.[89]

[88] History of FIDO Alliance, FIDO Alliance

[89] See Login with Fido

2.9.9 Applicable Industry Standards

FIDO Alliance[90] website provides publicly available statistics on implementations and use.

FIDO capability has been implemented by major technology vendors and incorporated into a variety of products (Figure 9).

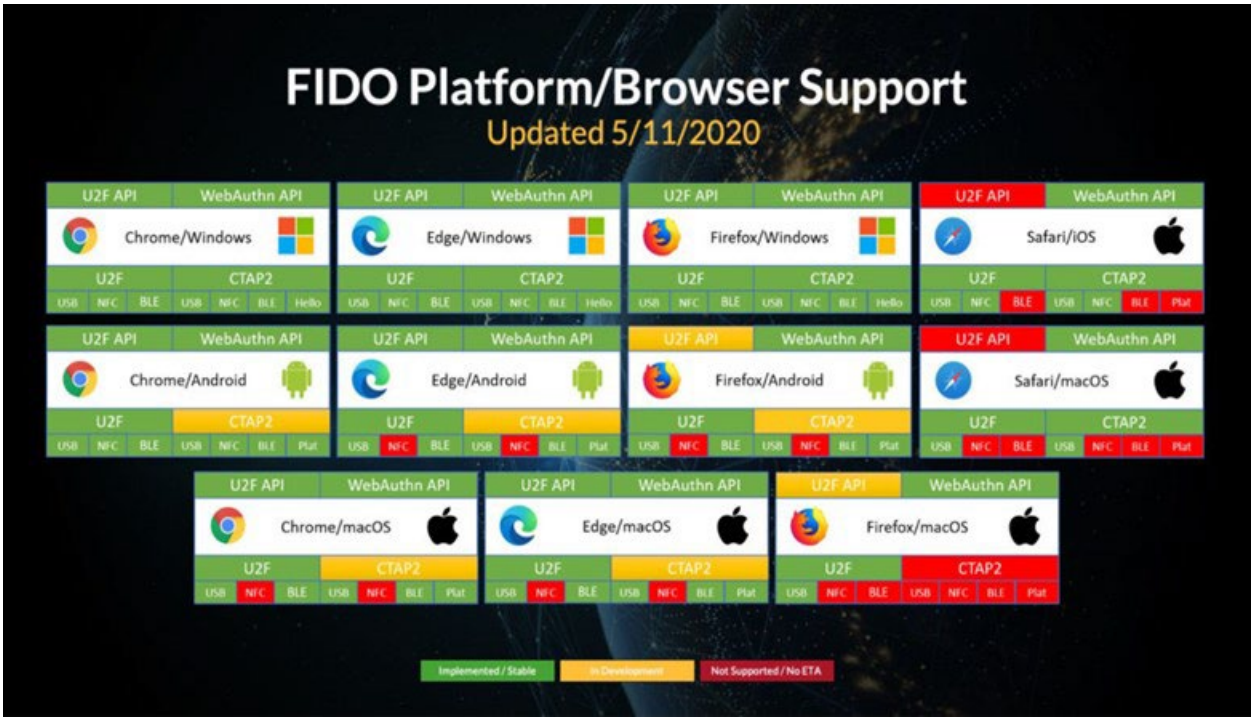

Figure 9. Support for FIDO2: WebAuthn and CTAP Browser and Platform Adoption Status Across Various Platforms[91]

Furthermore, examples of use cases[92] that leverage FIDO standards and a list of companies and organizations implementing FIDO[93] are available on the FIDO website.

[90] FIDO UAF Architectural Overview, FIDO Alliance, February 2017
[91] FIDO2: Web Authentication (WebAuthn), FIDO Alliance
[92] FIDO Case Studies FIDO2: Web Authentication (WebAuthn)
[93] Commercial Deployments, FIDO Alliance

2.10 W3C WebAuthn API

2.10.1 Definition/Description

The World Wide Web Consortium (W3C) is an international consortium where member organizations work to develop internet standards, primarily through creation of guidelines designed to ensure long-term growth and stewardship for the internet. Over 400 organizations are members of W3C, including FIs and payment networks. Open W3C standards aim to reduce payment provider and merchant costs, improve consumer choice and transparency, and create new opportunities to introduce value-added services.

WebAuthn is an API that makes it very easy for a relying party, such as a web service, to integrate strong authentication into applications using support built into all leading browsers and platforms. Web services can offer their users strong authentication with a choice of authenticators such as security keys or built-in platform authenticators such as biometric readers, instead of just a username and password.[94]

The WebAuthn standard is a widely accepted W3C specification developed in concert with FIDO, Yubico, Google, Mozilla, Microsoft, and others. It is a core component of the FIDO Alliance FIDO2 Project.

2.10.2 Applicability

The WebAuthn API enables communication between the browser and client about external or platform (embedded) authenticators. It is a two-party interaction. Using an API incorporated into the browser, WebAuthn standardizes the cryptography-based authentication process across multiple browsers and authentication methods to facilitate adoption:

- On-device (laptop/desktop) authentication with embedded trusted execution environment (TEE)[95] that stores private keys and authenticates the device directly to FIDO server.
- Remote authenticators (e.g., USB), that store private keys for authentication and use across multiple computers.
- Platform authenticators, with embedded fingerprint readers in laptops that can identify users (limited to dedicated biometric input devices).
- OOB authentication on a mobile device, using the standardized WebAuthn framework to accept authentication through a secondary device, e.g., tap to approve, PIN entry or biometric modalities (e.g., Touch ID), depending on whether low-risk or higher-assurance authentication is needed.

All major browsers are on track to implement full WebAuthn APIs. Chrome, Edge, Mozilla, and Safari support WebAuthn APIs now.

[94] What is WebAuthn? - Yubico, 2022.

[95] A trusted execution environment (TEE) is an area on the main processor of a device that is separated from the system's main operating system (OS). It ensures that data is stored, processed, and protected in a secure environment. If the main OS is compromised, the secure OS remains intact. What is a Trusted Execution Environment (TEE)? Definition from WhatIs.com (techtarget.com)

2.10.3 Technical Features

WebAuthn is an API that simplifies the ability of a relying party, such as a web service, to integrate strong authentication into applications using support built into all leading browsers and platforms. By using WebAuthn, web services can offer their users strong authentication with a choice of authenticators such as security keys or built-in platform authenticators such as biometric readers.[96]

Servers integrate with strong authenticators built into devices, such as Windows Hello or Apple's Touch ID. Instead of a password, a private-public key pair[97] (credential) is created for a website. The private key is stored in a secure area of the user device. The public key and randomly generated credential ID are sent to the server for storage. The server uses that public key to validate the user's identity.

WebAuthn uses FIDO authenticators, which provide all the benefits of FIDO. See Section 2.9 FIDO for more details.

2.10.4 How the Technique Works[98]

The following process describes authenticating a user on a website:

- The relying party generates a challenge and supplies the browser with a list of credentials registered to the user. It can also indicate where to look for the credential (e.g., on a local built-in authenticator, or on an external one over USB or BLE).
- The browser asks the authenticator to sign the challenge.
- If the authenticator contains one of the given credentials, the authenticator returns a signed assertion to the web app after receiving user consent.
- The web app forwards the signed assertion to the server for the relying party to verify.
- Once verified by the server, the authentication flow is considered successful.

[96] What is WebAuthn

[97] Private-public key pairs are long, randomly generated numbers that have a mathematical relationship with each other. Key pairs can only be used for a specific origin, like browser cookies, mitigating threat of phishing. WebAuthn Guide

[98] Web Authentication API, W3.org
Enabling Strong Authentication with WebAuthn, Chrome

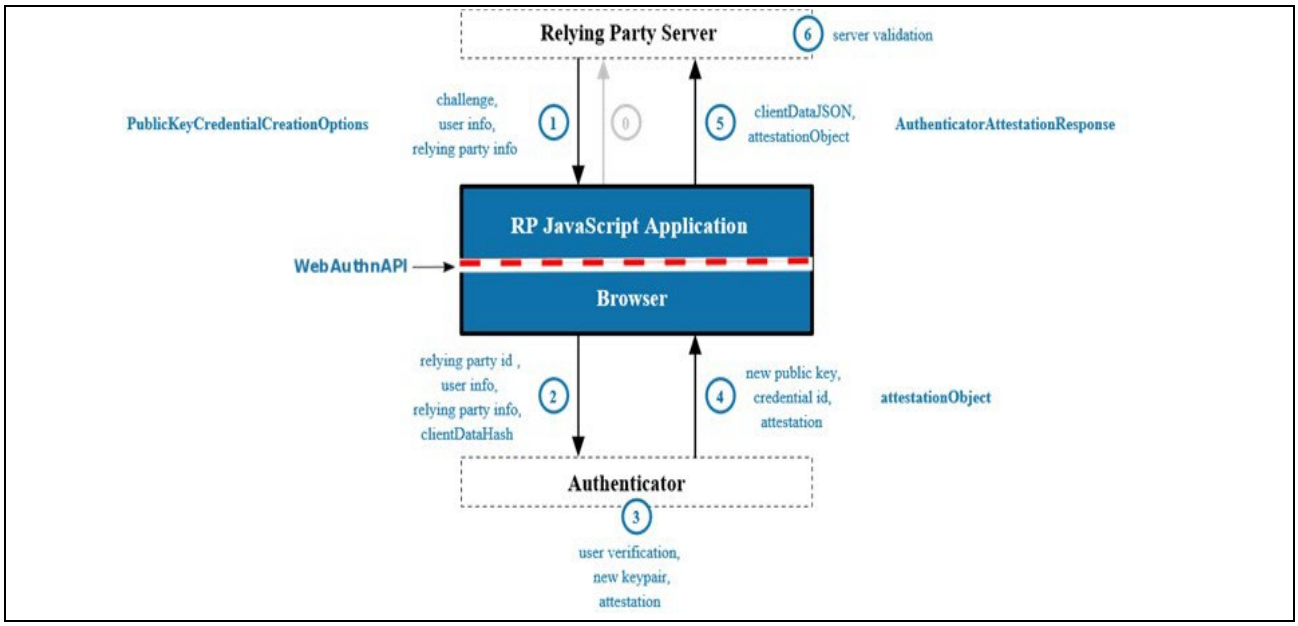

Figure 10. WebAuthn Authentication Flow[99]

Browsers can accept biometric authentication from a user's device when the user is shopping or making payments online. For example, the user logs into a website using fingerprint or facial recognition, not a username/password. If used with a 'Pay' wallet, biometric data remains in a secure area of device.

For ecommerce, the standard lets retailers offer their consumers the option of using a biometric login when registering for the first time. Since no passwords are saved online, they cannot be stolen if the database is breached.

To register with WebAuthn, the server provides data that binds a user to a credential (i.e., the public/private key pair). Data includes identifiers for the user and organization. Risks Associated with the Technique

WebAuthn relies on FIDO authenticators and inherits all associated risks as outlined in *section 2.9.5*.

2.10.5 Consumer Impact/Level of Friction

The process does not require consumer action other than registration and requires no password for the consumer to remember, reducing the friction of authentication. WebAuthn is built-in as the platform authenticator for Android and iOS. Additionally, consumers can plug hardware authenticators into mobile devices via USB/USB-C/Lightning connectors.

[99] Web authentication: An API for accessing Public Key Credentials Level 1, W3.org. This document has been reviewed by W3C Members, by software developers, and by other W3C groups and interested parties, and is endorsed by the Director as a W3C Recommendation. It is a stable document and may be used as reference material or cited from another document.

2.10.6 Implementation Considerations

WebAuthn works in tandem with other industry standards such as credential management and FIDO 2.0 Client to Authenticator Protocol 2 (CTAP). CTAP is an application layer protocol used for communication between a client (browser) or a platform (operating system) and an external authenticator, which can roam between devices.[100]

Furthermore, WebAuthn can match the assurance of the authenticator to the riskiness of the activity where possible. For example, for very high-risk transactions, a FIDO level 2 or higher certified authenticator may be advisable to provide additional assurance for a mobile browser transaction using technologies such as NFC. This is accomplished by the relying party examining the authenticator's attestation object to match against FIDO authenticator vendors and models that are acceptable for a specific transaction.

Because FIDO authenticators can be shared physically among individuals, the use of MFA, such as biometrics or KBA where possible, to identify the specific individual operating the device should be considered.

2.10.7 Maturity and Effectiveness of Tool

WebAuthn is now shipping in all major browsers on both desktop and mobile platforms. The technique is an improvement on password-only authentication.

FIDO and EMVCo are working to deliver a solution to enable the WebAuthn API to support EMV 3DS and SRC use cases.[101]

2.10.8 Applicable Industry Standards

W3C coordinates standards development with TC68, EMVCo (tokenization, SRC and 3DS), FIDO, X9 and ISO 12812 (MFS).

2.10.9 Publicly Available Statistics on Implementations and Use

- W3C
- WebAuthn: W3C technical reports index

[100] See WebAuthn Developer Guide, Developers Yubico

[101] EMVCo and the FIDO Alliance to Address FIDO Authentication in EMV® 3-D Secure Use Cases, Fido Alliance, June 2018

3. Device Authentication

Device authentication (also known as endpoint authentication) is a dynamic security mechanism designed to ensure that only authorized devices can connect to a given network, website, or service (e.g., banking or payment app) by verifying the user ID linked to the mobile device and one or more authentication methods for secure access. Device authentication is often used in conjunction with user authentication for greater security. Authenticating both the user and the device can provide two-factor authentication (2FA). There are special mobile phone apps that provide one-time password tokens, allowing the phone itself to serve as the physical device to satisfy the possession factor. The password response sent from the registered device verifies that the user is connecting from an authorized endpoint. Dynamic cryptograms generated from the authorized mobile device validate the card data stored in the phone.

3.1 Dynamic Cryptogram

3.1.1 Definition/Description

EMV chip transactions use transaction information presented from the debit or credit card data stored in the mobile wallet and the terminal to create a one-time-use dynamic cryptogram that is sent in the authorization message with the data that was used to create the cryptogram. The cryptogram is generated using secret keys that are stored on the payment device.

3.1.2 Applicability

The issuer uses the cryptogram to validate the authenticity of the payment device.

3.1.3 Technical Features

The payment device generates a dynamic cryptogram using the securely stored secret key. Information used to create the cryptogram includes transactional data, such as amount, time, and date, as well as a terminal unpredictable number and device information. The payment device then uses its secret key to generate the cryptogram. The cryptogram and the data used to create it are sent in the transaction message to the issuer. The issuer uses a copy of the secret key to authenticate the cryptogram received from the device indicating if the payment device is genuine, thereby protecting against counterfeit fraud. An important feature of the cryptogram is that it is valid only for a single-time use, so even if an eavesdropper captures the transaction, it cannot be rerun.

Figure 11 and **Figure 12** show how a dynamic cryptogram is created using dynamic data and other fields, which are stored in data element 55.

Figure 11. What Is Dynamic Data?[102]

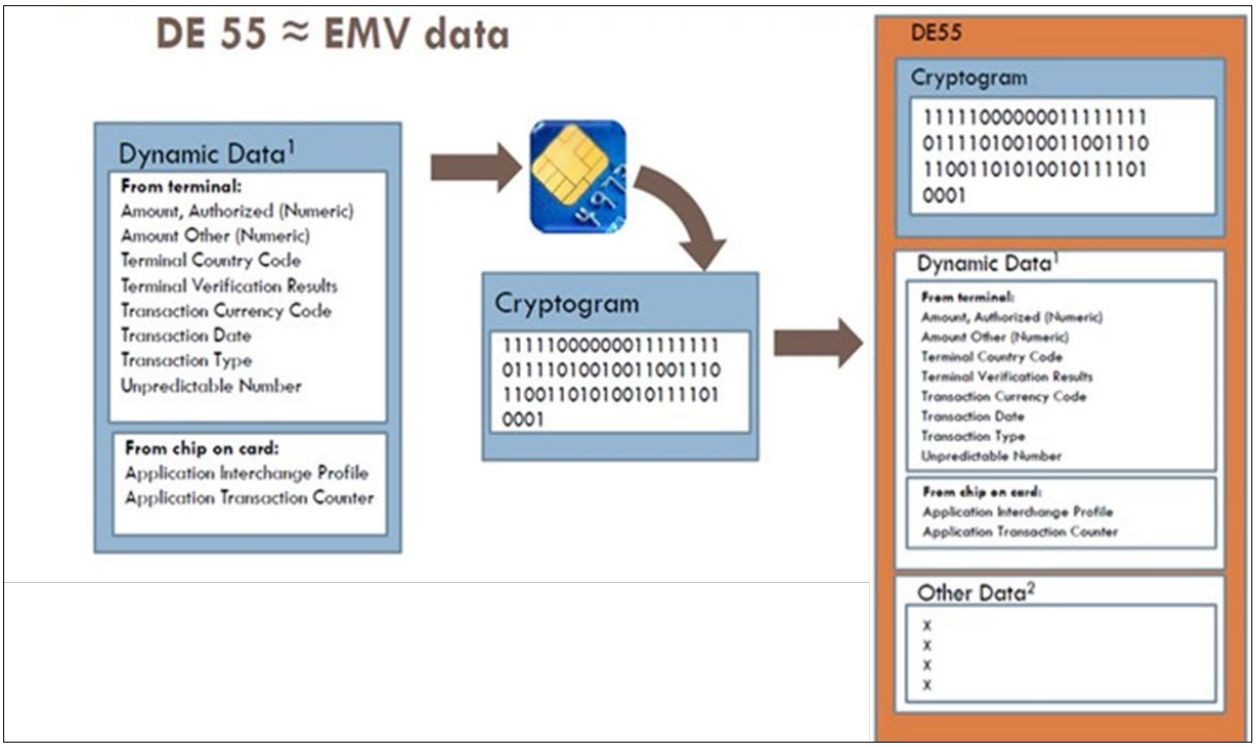

Figure 12. Dynamic Cryptogram Creation[103]

[102] Image provided by and used with permission from Visa.
[103] Dynamic Data used to create cryptogram defined in EMVCo v4.3 specification, Book 2, page 88. Other data is used for illustrative purposes and does not fully represent other data sent in DE55.

3.1.4 How the Technique Works

Using the dynamic cryptogram is a standalone process. The mobile device sends the device-generated cryptogram and data that was used in creating the cryptogram to the issuer. The issuer creates its own cryptogram using the same data that the chip used and the same key. The issuer then compares the two cryptograms, and if they are the same, the device is genuine.

3.1.5 Risks Associated with the Technique

This technique has some associated risk. The data used to create the cryptogram is sent with the cryptogram in the authorization message to the issuer. The issuer uses the data to create its own cryptogram for comparison with the cryptogram received from the device. This data may be in the clear if it does not follow the PCI standard which recommends (not requires) that EMV transactions in flight and at rest be encrypted, however the card number is tokenized for mobile transactions, with the token replacing the PAN in the transaction. Similarly, for an in-app transaction (also tokenized), the cryptogram is created and sent in the transaction for the issuer to process.

3.1.6 Consumer Impact/Level of Friction

Dynamic cryptograms have no consumer friction because the cryptogram is generated during device presentation.

3.1.7 Implementation Considerations

All payments stakeholders are involved in implementing dynamic cryptograms. The application on the device must be able to generate the cryptogram. The merchant must enable the terminal to process a payment network's EMV chip cards. The issuer/issuer processor must manage the keys put on the card and validate the cryptogram during the transaction.

The dynamic cryptogram is available on all chip-capable cards/mobile devices.

3.1.8 Maturity and Effectiveness of Technique

This technique is well-established. Dynamic cryptograms have been used for over 20 years.

EMV chip cards with dynamic cryptograms have decreased counterfeit fraud by 87%[104] at EMV-enabled merchants. However, the EMV chip and dynamic cryptogram do not protect against CNP fraud.

3.1.9 Applicable Industry Standards

Various industry standards and specifications are used in the implementation of this technique, including those managed by X9, ISO, EMVCo, GSMA, PCI SSC.

The payment networks define the cryptogram generation algorithms.

3.1.10 Publicly Available Statistics on Implementations and Use

See Worldwide EMV Deployment Statistics - EMVCo

[104] Visa: Chip Cards Reduce Counterfeit Fraud by 87%, Pymnts.com. September 2019

3.2 MNO Risk Scoring, Phone Number Validation, Device Binding and MNO Intelligence

3.2.1 Definition/Description

These techniques involve various technology stacks and protocols to capture data about/from the consumer or the consumer mobile device to validate the data against existing attributes stored in the mobile network operator (MNO) database.

MNO intelligence adds another layer of verification by checking further attributes such as account ownership, network status or recent activities on the account. Device binding links and registers the device attributes captured at initial enrollment to the user account. This information helps to determine device eligibility to access certain services at later stages.

These techniques are primarily offered by data aggregators, who can connect in real time to different MNO databases to validate consumer and device attributes, and to help with phone identification and/or consumer authentication processes required during onboarding or initiating transactions from a mobile phone. Such data aggregators usually connect to other service provider databases (e.g., utility providers or government accessible databases) to expand their coverage and enhance their matching scores. In some countries, MNOs collaborate to establish joint venture entities to act as data aggregators.

3.2.2 Applicability

This technique is used primarily for remote enrollment or payments where the user is not pre-registered (e.g., money transfer or topping up prepaid accounts).

The technique is designed for issuers, merchants, and payment, electronic funds transfer (EFT) and money transfer processors.

3.2.3 Technical Features

MNO risk scoring verifies consumer account attributes against data that is stored with the MNOs. Capabilities depend on the MNO capabilities and consumer account details (e.g., a prepaid account may not have full consumer attributes like name and address) that will define the overall data to be verified and the test cases to be executed. MNO intelligence sits on the top of such verification and adds further analytics and logic to utilize account or user attributes.

Phone number validation and other device attributes usually rely on existing protocols defined by GSMA to exchange device attributes through the carrier network and run the corresponding verifications to enhance the overall risk score (e.g., device type or carrier-network-based location).

Other Key Characteristics

In addition to basic account details, other attributes such as account status, wireless vs. wireline detection, and geographic location of the MNO can help the risk-scoring system provide the final assessment based on comprehensive checks.

The use of GSMA Mobile Connect® (Figure 13) can enhance the use cases where consumer possession of the mobile device or a two-factor authentication is required. By matching the end user to their mobile phone number, Mobile Connect empowers the user to confirm his/her identity online, and authorize transactions such as payments, sharing only the personal data needed to complete the transaction.

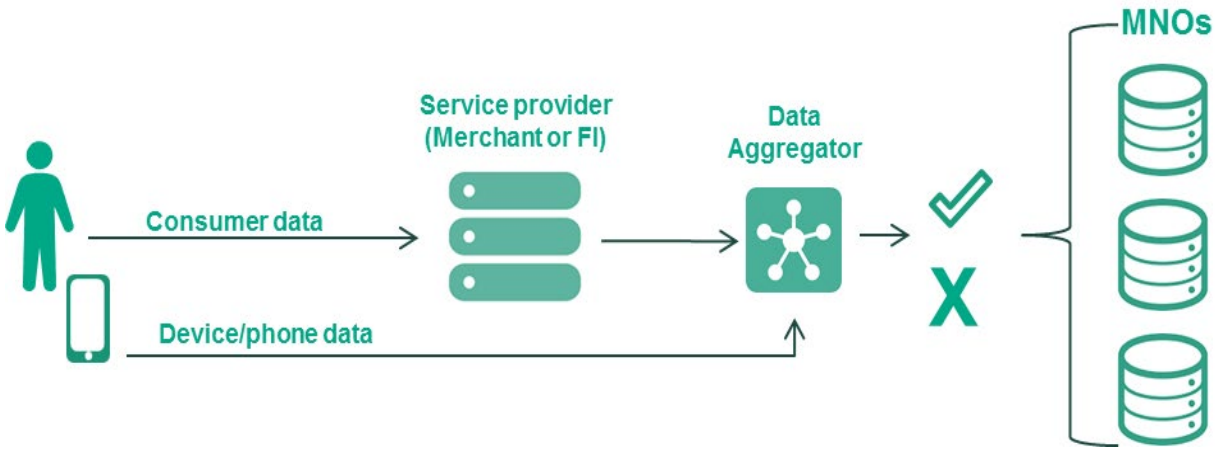

Figure 13. GSMA Mobile Connect[105]

3.2.4 How the Technique Works

How this technique works usually depends on the carrier, aggregator (e.g., Payfone, Boku, Danal), device capabilities, and the expected interaction from the consumer. For example, validating the phone number can be done using different techniques including:

- A mobile-originated SMS can be triggered automatically (if supported by the operating system and permissions are granted), which will be transparent to the consumer.
- The consumer may be instructed to send an SMS to a short code which uses the same technology but will require an action from the consumer.
- Header Enrichment may be used to validate the phone number and/or other attributes transparently via data fields within the HTTP message header without direct consumer interaction.

Some use cases match data against the MNO consumer database by deploying an API that has advanced techniques to lookup information in different databases in real-time and adds some analytics to offer more intelligence to the decision-making. The API request made by the authenticating party specifies what data should be returned in the authentication request. In most cases, a consumer must consent to the user of the service either explicitly or as part of language integrated into the terms and conditions of a service agreement.[106]

Device binding involves capturing device vectors, which may be hardware values (hardware vectors) or software or OS-specific values (soft vectors) during initial app installation and enrollment. This device fingerprint will be used to adequately ensure the possession status and device eligibility for accessing certain functions. See Figure 14.

[105] Mobile Connect, GSMA

[106] Specifics on consent and available consumer information vary by carrier and aggregator as well as consumer device and account type. For further information, please see specific aggregator documentation e.g. Prove or Boku as examples.

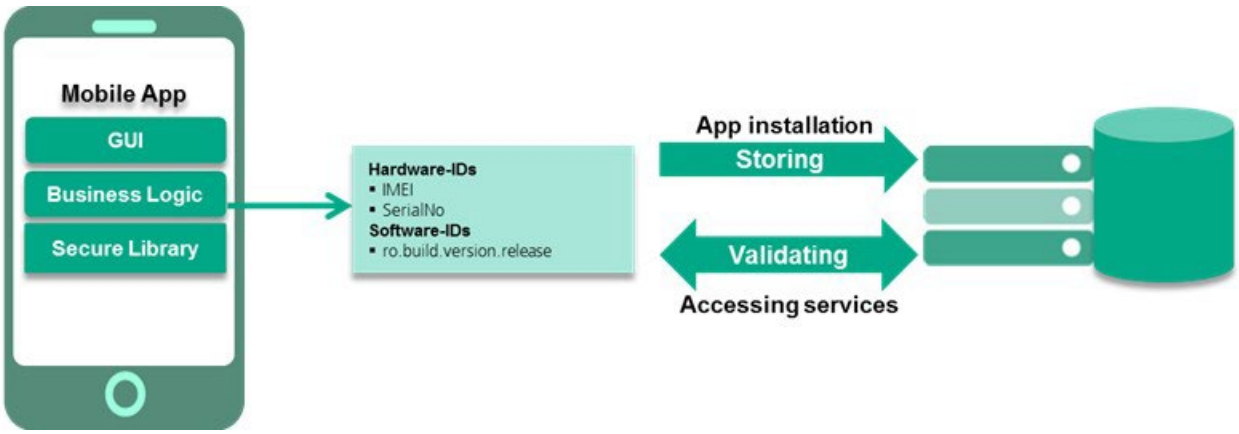

Figure 14. GSMA Device Binding[107]

3.2.5 Consumer Impact/Level of Friction

The consumer might be prompted to submit consent to access their MNO account details during the verification process. This could raise security concerns or add a level of friction.

3.2.6 Implementation Considerations

Implementation typically occurs via a well-defined API call to a data aggregator who handles the complexity of data lookup and further MNO communication. The primary consideration for adopting MNO risk scoring is to validate the coverage of the data sources that will be used, as well as to ensure that the right consents are presented to the end consumer during the verification process.

3.2.7 Maturity and Effectiveness of the Technique

This technique is a commercially available solution in the marketplace. Usage could be impacted in some countries where regulations require further geographical limitation or other security practices to be implemented.

Because MNO risk scoring relies on the consumer having an existing account in the MNO database, coverage does not include all consumers. This affects prepaid mobile consumers in particular who are not covered by Know Your Customer (KYC) regulation (in the U.S. and possibly other countries) as well as corporate accounts where individual consumer information may not be available.[108] Phone number and other device attributes limit the use case to the mobile channel; devices connected to the internet outside of the GSM network (e.g., using a PC or tablet) will not qualify.

3.2.8 Applicable Industry Standards

- Secure communications use GSM, HTTP and SSL standards.

3.2.9 Publicly Available Statistics on Implementations and Use

Statistics are not available for this technique.

---

[107] Mobile Connect, GSMA

[108] For prepaid cards without reloadable and credit/overdraft features, such as closed-loop prepaid cards and gift cards, the "customer" for purposes of the Customer Identification Program (CIP) rule is the third-party program manager who has the pooled account at the bank. In these instances, the bank (or its agent) does not need to identify and verify each cardholder, but rather implement its CIP on the third- party program manager who holds the pooled account, ICBA.

4. Risk-Based Authentication (RBA)

Risk-based authentication is a mechanism that enables an issuer to implement frictionless payments for low-risk transactions. It can be static or adaptive and may incorporate contextual authentication.[109] The issuer uses a risk engine and set of risk rules to determine whether the transaction is deemed safe or if an additional (i.e., step-up) authentication challenge is required. RBA occurs in the background, eliminating consumer friction unless step-up occurs. Issuers may implement their own RBA algorithm or use third-party vendors to implement the risk engine.[110] For example, EMV 3DS uses RBA.

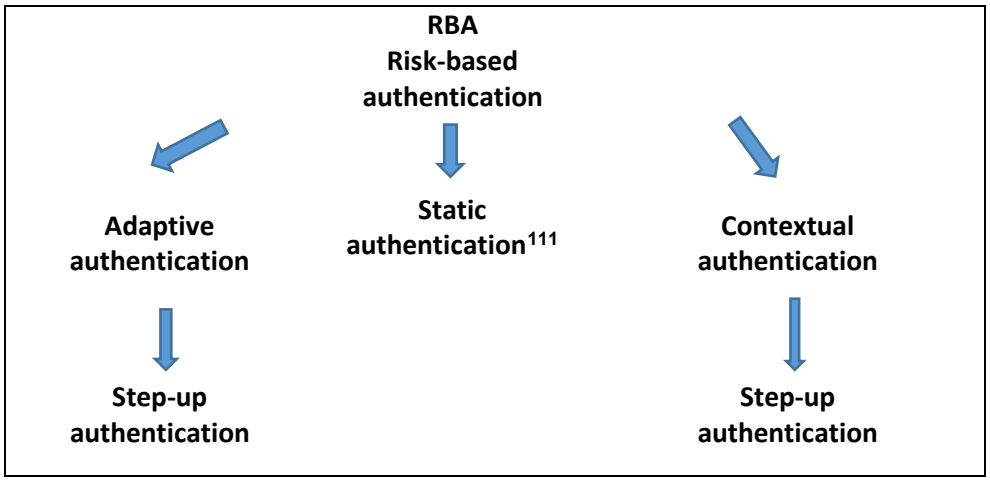

Figure 15. Types of Risk-based Authentication

[109] Contextual-based authentication uses logic-based mechanisms, such as geolocation, time of day, IP address and device identifiers, to determine whether a user should be required to use a second factor based on policy. For example, a customer uses a password to sign on to a banking site and then wants to transfer money. If that customer signs on from the U.S., the MFA system might not require further action. However, if they sign on from Uzbekistan, the system might require a second authentication factor. Ultimate guide, Ping Identity, 2020

[110] Modirum 3-D Secure, Modirum

[111] Static authentication reuses a specific authenticator (e.g., static password). This type of authentication only provides protection against attacks in which a fraudster cannot obtain the authenticator. The strength of the authentication process is highly dependent on the difficulty of guessing or decrypting the authenticator values and, therefore, how well protected they are in transit and while stored on the system. "Guide to selecting information technology,"

4.1 Adaptive Authentication

4.1.1 Definition/Description

Adaptive authentication (AA) is a type of RBA. RBA enables issuers to challenge only those transactions considered to be a fraud risk through transaction risk analysis. RBA measures risk associated with a user login and payment transaction activities based on information about a user's device, login patterns and other risk indicators, and calculates a real-time risk score for any access attempt, based on a pre-defined set of rules. The risk score determines the risk level, which measures if the login attempt is legitimate or likely to be fraud. RBA then presents the user with authentication options appropriate to that risk level. Users receive a challenge only when the system identifies an activity as high risk, it appears unusual for the end user, or it violates an organizational policy. A challenge may require step-up authentication by asking the user to answer additional questions (e.g., KBA) or receive an out-of-band OTP to complete the authentication.

Adaptive Authentication is dynamic. It works by selecting appropriate authentication factors depending on a user's risk profile and tendencies, as well as specific transaction data (e.g., amount). AA therefore adapts the type of authentication to the situation. The adaptive feature minimizes friction and establishes trust among the transaction, the identity, and the device during the payment journey. Depending on the situation, AA may ask for different levels of assurance, enabling it to tighten security when the risk is deemed higher. This approach is unlike standard authentication methods, including MFA, that ask users for specific credentials whenever they try to login to an account or access corporate resources.

Adaptive Authentication intelligently changes requirements, making it much harder for a hacker to gain access to an enterprise because some of the signals used are difficult for an attacker to circumvent. This enables organizations to define security levels based on existing risk.

At the transaction risk level, AA evaluates multiple parameters, which may include characteristics of the user device, browser, and other attributes; malware detection; geolocation; IP address; consumer use of the mouse and/or keyboard; or other behaviors displayed by the consumer. The level of complexity depends on the risk associated with the transaction. If the risk is considered low, username and password may be acceptable for authentication. If the risk is high, then additional authentication methods are applied to prove that the user is who he or she claims to be. AA tries to balance the amount of potential fraud loss with loss of a consumer who has a bad experience. AA is even more secure and flexible when evaluating contextual, behavioral, and correlated data, providing a more informed decision and a higher level of assurance about the user identity.

Using dynamic policy decision-making, AA only permits access if the level of assurance exceeds the level of risk associated with the context of the request. The dynamic nature of AA policy decisions differentiates it from traditional authentication approaches. Dynamic policy controls can be device-based, behavior-based, resource-based, or network/browser-based.

With advances in technology, changing authentication landscape, and increased number of data points, institutions have more tools to help reduce false positives, and identify fraud that they did not catch in real time, without a major impact to consumers. Use of these tools is what makes the approach adaptive.

4.1.2 Applicability

Adaptive Authentication is an omni-channel approach that applies to multiple types of implementations, including online banking, chat support, mobile banking, call center, interactive voice response (IVR), and third-party services, and to multiple channels (e.g., mobile, internet, Internet of Things [IoT]).

This adaptive approach can support multiple payment methods (e.g., card, wire, Automated Clearing House (ACH), as well as in-app or with a mobile browser, depending on the solution. It is typically used during account creation, during the provisioning/enrollment process, or during transactions, and can support either consumer verification or device authentication.

FIs, processors, payment networks and merchants include AA as part of a layered approach.

4.1.3 Technical Features

While AA tools follow the same principles, the approaches, expertise, and integration of key security technologies vary widely across solutions. Solutions may include open, cloud-based architectures, integration of third-party tools and data, risk analytics engine, and machine learning algorithms. Rules are adjusted dynamically based on emergent user behavior patterns.

Machine learning (ML)[112] algorithms in these tools monitor and learn user behavior over time to build a more accurate profile. They may track devices, typical user login times, or usual work locations. They check IP addresses and network reputations, in addition to threat data for those networks. AI can monitor in real time and identify anomalies in the user's authentication patterns or threats in the authentication path (such as compromised networks). ML and AI enable organizations to collect and analyze data to make smarter real-time decisions about whether to approve, block, or reject the transaction.

AA risk analytics may leverage user, device, and app data from mobile device, including OS version, device ID, geolocation, jailbreaking/rooting, and app security data points (e.g., malware detection) to provide a measure of trust.

Risk score assignment is based on behavior and context, with the response to the perceived risk based on rules established by organization. These rules may vary by risk score, user role, location, and device.

4.1.4 How the Technique Works

Adaptive authentication happens in the background, constantly collecting behavior data online or from mobile channels, including additional consumer data. The authentication server performs real-time risk analytics with machine learning and customized rules to build a dynamic model. From the analytics, AA develops a risk assessment and, if it recognizes an anomaly in behavior, flags the transaction as potentially risky.

The adaptive approach collects other data on the server to complete the picture, including data from third-party applications. All information comes together in the authentication server, where ML helps to mitigate fraud schemes and otherwise act on anomalies. ML algorithms can analyze millions of data points collected, including other uses and channels and create a real-time data model for any suspicious activity.

[112] Machine learning is part of artificial intelligence.

Adaptive authentication determines what security measures to apply, based on the risk score. If the score is low, no additional steps are required. All steps are transparent to the consumer unless additional data is needed, for which the consumer is prompted to authenticate his/her identity. Applying the appropriate level of security/friction for each transaction ensures a positive consumer experience.

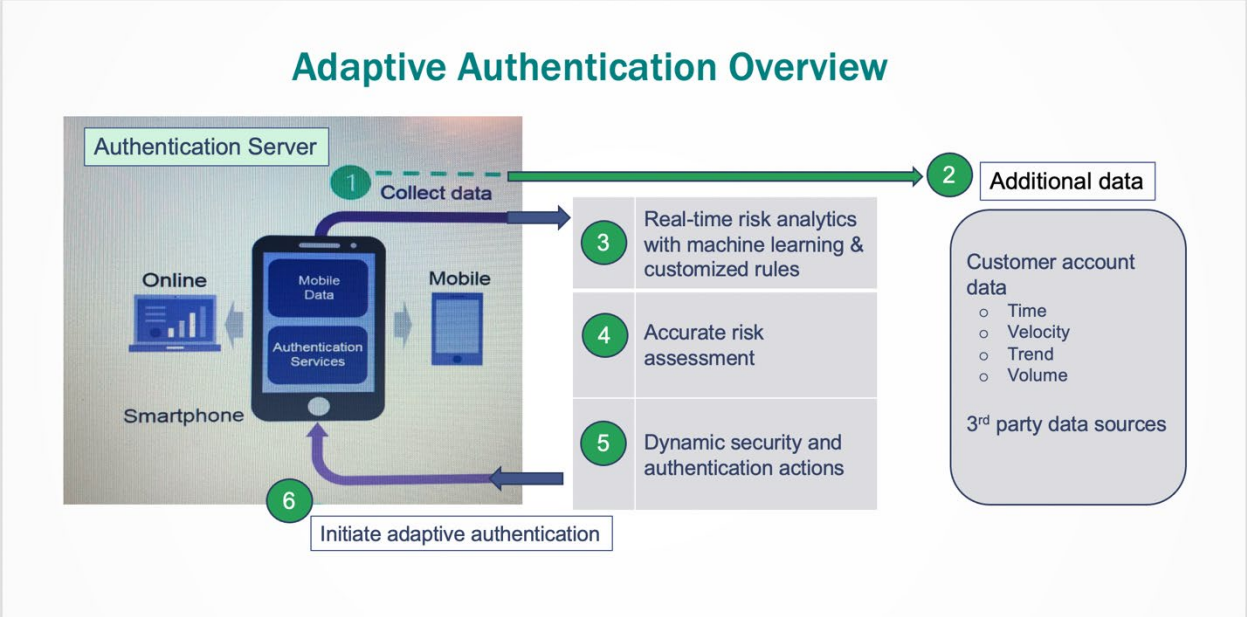

Figure 16. Example of Adaptive Authentication Flow[113]

Figure 16 illustrates an example of AA flow. Steps 1-5 are real-time, transparent to consumer.

The authentication server collects comprehensive data on device and app integrity, user behavior, and other contextual data across online and mobile channels (on the client side). The server collects additional consumer data from online/mobile banking applications and services, and third-party services to complete the picture. The server/risk analytics engine brings together all data and uses machine learning and customized rules to identify fraud schemes and anomalies in real time.

Rules are adjusted dynamically based on emergent user behavior patterns. ML algorithms help analyze potentially large number of data points across uses/channels. The system creates a real-time data model/risk score to look for suspicious activity. The risk score is calculated from behavior and context, and rules established by organization, which may vary by risk score, user role, location, and device. The risk review determines the needed dynamic security and authentication actions based on the risk level determined by the risk score. If the risk score is acceptable, there are no additional steps.

Additional security measures prompt the consumer to authenticate. For example, if the user tries to access the website or app using an unregistered device, the user is prompted to register the device. If the login is from a different geographical location, the user may need to answer a security question or receive an OTP. Depending on the scenario, the system may block the user from access, or receive a challenge to prove identity. The user responds to the appropriate adaptive authentication method.

[113] "Enable Seamless, Secure Access with Adaptive Authentication." Adaptive Authentication and Authorization | Ping Identity 2017

4.1.5 Risks Associated with the Technique

While adaptive systems provide an added layer of protection, they do not replace other authentication methods that are necessary to log in and initiate a transaction, so users still need to use passwords.

4.1.6 Consumer Impact/Level of Friction

Consumer impact is minimal. Adaptive Authentication can request less information from users who are recognized and behaving in expected ways and only query users for more information if needed, when circumstances suggest a greater security risk. This means fewer interruptions for users and lower barriers of entry, where improved customer satisfaction is worth the trade-off with tighter security.

Adaptive authentication allows differing consumer paths, depending on the output of various risk models. It can be used with strong authentication techniques, e.g., push authentication from a mobile device, OTP, time-based OTP, FIDO, biometrics (e.g., fingerprint), to provide risk-based MFA.[114]

4.1.7 Implementation Considerations

Implementation considerations will vary depending on the level of customization needed by organizations when developing rule sets vs. using turnkey rule sets. The AA implementation may provide APIs or a user interface for a single point of entry for rules, workflows, and actionable authorizations. AA can be updated as new threats and risk factors are identified; they can also be added to scoring and comparison processes.

FIs can talk to industry security consultants and vendors to determine whether to develop or buy/customize a solution and ensure the solution covers multiple digital channels on day one.

Adaptive authentication has several implementation challenges, including:

- Many disparate tools make it challenging to coordinate security effectively. Institutions need to get the appropriate technology tools deployed in a timely manner.
- FIs still have many legacy systems and processes tied to passwords and usernames
- Authentication is not one-size-fits-all, with multiple devices requiring authentication.
- Invoking authentication at the right level and using the right type of authentication at the right time may be difficult.

4.1.8 Maturity and Effectiveness of the Technique

Implementation of AA is just starting to gain traction, but it is not a new concept. Technology advances in the authentication landscape, increased number of data points, and concern about consumer friction are driving implementation, with the industry creating new AA solutions to decrease false positives and identity fraud in real time.

Integrating data from other FIs and external sources helps to improve the AA analysis. Leveraging existing tools (e.g., MFA) can make the implementation more cost-effective. However, the process can be complicated, and smaller FIs and merchants may need to work with third-party processors

Many available solutions support AA, but the market may be fragmented. It includes vendors of all sizes and disciplines.

[114] Adaptive Authentication, RSA

4.1.9 Applicable Industry Standards

- X9 TR 48-2018[115] section on risk-based authentication. This specification explains how issuers, merchants and applications can use RBA to determine the level and complexity of authentication methodologies to achieve a satisfactory level of confidence that user is the legitimate consumer.

4.1.10 Publicly Available Statistics on Implementations and Use

According to a Research and Markets January 2021 report,[116] the risk-based authentication market was valued at USD 2.22 billion in 2020 and is expected to reach USD 5.13 billion by 2026, at a CAGR of 15% over the forecast period 2021 - 2026.

4.2 EMV 3-Domain Secure

4.2.1 Definition/Description

EMV 3-Domain Secure (3DS) is a global risk-based secure messaging protocol that consists of three domains: merchant/acquirer domain, issuer domain, and interoperability domain. 3DS enables issuers to authenticate consumers in real-time during an online or mobile-initiated transaction to reduce fraud and cart abandonment, improve approval rates, and accelerate growth in ecommerce. It can also verify identity for select non-payment activities, such as adding a payment card to a digital wallet.

The initial version of 3DS (v1.0), launched in 1999, only supported ecommerce transactions and required active cardholder enrollment. Version 1.0 also challenged 100 percent of transactions, requiring consumers to remember and enter a static password or answer KBA questions during the online process for every purchase. This process created a poor consumer experience and led to high cart abandonment. As a result, merchant adoption in the U.S. was very low.

In 2017, EMVCo published 3DS (v2.0) that applies an RBA approach. Issuers and merchants exchange additional risk data at both the ID&V and transaction levels to assist issuers with authentication decisions. EMV 3DS incorporates risk-based elements and delivers expanded capabilities in terms of technology, security (e.g., tokenization), performance, user experience and flexibility. It also provides many more data points to help with the risk analysis, including cardholder and device data exchanged between the merchant and the issuer to assess whether to authorize the transaction or challenge the consumer for further verification. Merchants collect information to exchange with issuers to authenticate the cardholder's identity before authorization occurs. They supply data such as:

- Cardholder account information; merchant risk indicator; pre-authorization, payment, cardholder, and shopping cart information
- Device ID, geolocation, email address, mobile phone number, shipping, billing, and IP addresses

EMV 3DS provides faster authentication, improved latency, and improved response time, with fewer false positives, fewer chargebacks to manage, and decreased call center costs related to password reset. Merchants choose when to invoke EMV 3DS, giving them more control, and enabling them to focus their resources on monitoring potentially fraudulent transactions.

[115] X9.org

[116] Risk-based Authentication Market - Growth, Trends, COVID-19 Impact, and Forecasts (2021 - 2026), Research and Markets, 2021

4.2.2 Applicability

EMV 3DS is applicable to credit and debit card-based mobile and digital payments, is device agnostic, and works across channels.

Use cases include:

- Mobile and internet browser purchases, mobile in-app purchases, digital (checkout) wallet
- Secure request of tokens for card-on-file (CoF) and IoT device implementations
- ID&V processes to verify identity as part of the tokenization process in mobile wallets

EMV 3DS is applicable for financial institutions/issuers, merchants, processors, networks, and consumers.

4.2.3 Technical Features

Risk-decisioning leverages a range of variables to classify the risk quotient for each transaction to make the authentication decision. EMV 3DS can exchange more than 150 data elements among the consumer, merchant, and issuer – 10 times more contextual data than 3DS v1.0. Data points are transactional, behavioral, and contextual. Advanced analytics use the data to make smarter authentication decisions. Machine learning helps to better assess the risk profile of the transaction and decide if a challenge is needed. All real-time analysis runs in the background, transparent to the consumers.

EMV 3DS operates with three interoperability domains to provide authentication messaging between the issuer, acquirer, and payment network.

- The interoperability domain contains systems, functions and messages that allow the issuer and acquirer domain systems to switch transactions and interoperate worldwide.
- The issuer domain contains systems and functions of the issuer and its consumers (i.e., cardholders). The issuer domain authenticates 3DS transactions.
    - The process includes the consumer device, which contains the merchant app or browser, and access control server (ACS).
    - The ACS verifies whether 3DS authentication is available for a particular card number and authenticates the cardholder for a specific transaction.
    - The merchant 3DS client is a consumer-facing component that allows the consumer to interact with a merchant for initiation of the 3DS protocol as part of the shopping experience. This can be application-based (using an integrated 3DS software development kit [SDK]) or browser-based.
- The acquirer domain contains systems and functions of the acquirer and its consumers (i.e., merchants). The acquirer domain initiates 3DS transactions.
    - The 3DS server is the functional interface between the merchant and 3DS messaging. It is responsible for ensuring that the Directory Server (DS) is a known payment system DS and that message contents are protected.
    - The payment system certificate authority (CA) distributes the DS public key to the 3DS SDK and generates transport layer security (TLS) certificates for the 3DS entities.
    - Authentication messages include authentication request; authentication response; challenge request (app- and browser-based); challenge response (app- and browser-based); results request; results response. This enables a three-way exchange of information, with all parties equally involved.

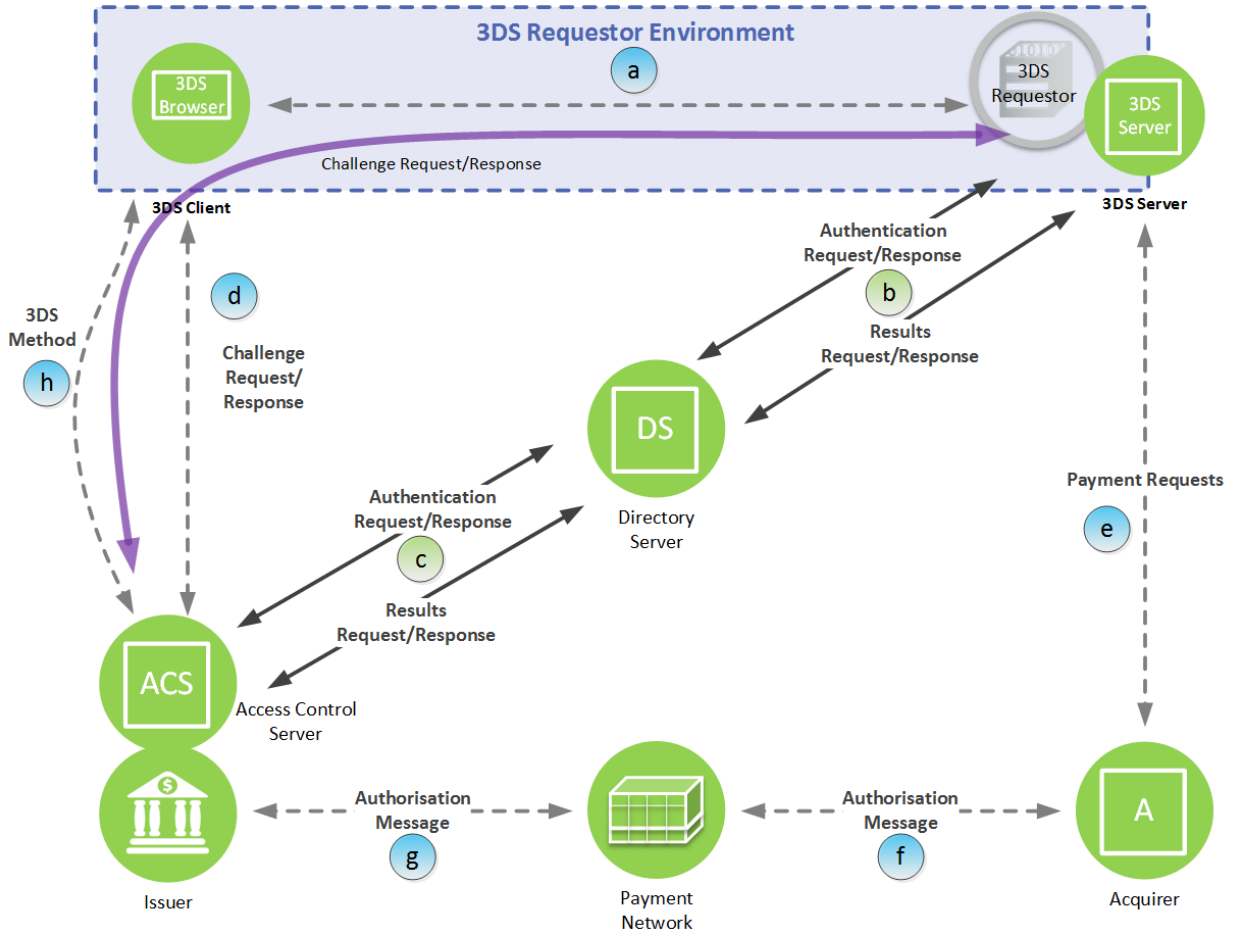

Figure 17. 3DS Domains and Flows[117]

4.2.4 How the Technique Works

The consumer initiates an online or mobile purchase and checks-out on merchant's mobile website. The merchant passes consumer purchase information, along with device data and other details to the Directory Server (DS) of the applicable payment network via a 3DS request.

The payment network routes the transaction to the issuer to authenticate the consumer and confirm purchase. The issuer can use risk-based and/or challenge authentication to confirm the consumer's identity. The issuer uses combined data points to assign a risk score to the transaction, performing a range of checks to ensure the consumer is legitimate and to decline expected fraudulent transactions.

The issuer reviews the risk score to determine the transaction risk level.

- If the risk is below the defined threshold, the issuer can approve the transaction without a consumer challenge.

[117] EMV 3-D Secure-Protocol and Core Functions Specification v2.0.0, Figure 2.1: 3DS Domains and Components, p.29. The specification is available, royalty free, from the EMVCo website.

- If the transaction is high risk (or required by country mandate/regulation), the issuer will request stepped–up authentication, (e.g., asking the consumer to validate his/her identity with an OTP or biometric option).

The merchant makes the final decision about whether to invoke 3DS and let the ACS process the challenge or complete transaction without additional authentication.

- With frictionless flow, the authentication process is integrated seamlessly into the merchant checkout and does not require any additional consumer interaction during process. The 3DS protocol enables data to pass between the merchant and the issuer that supports enhanced risk-based decision-making, minimizing need for challenge authentication. The consumer device data and payment information gathered in frictionless flow allow the risk-based decision to occur to authenticate consumer. Merchants may skip 3DS on a transaction-by-transaction basis and use their own risk models to decide how to proceed with the transaction.
- With a challenge flow, the merchant invokes 3DS. The ACS recognizes the challenge request during the frictionless flow, and transitions to challenge flow using a specific challenge method. Challenge methods include static, dynamic or OOBA (e.g., payment verification on the device via the issuer mobile banking app from the same consumer device), FIDO, OTP sent by text to the phone, and security questions (KBA) by the consumer.

Once the consumer is authenticated, the merchant continues processing the transaction.

4.2.5 Risks Associated with the Technique

A successful EMV 3DS implementation depends on the richness of data exchanged between the merchant and the issuer to achieve high authentication rates and identify legitimate fraudulent transactions.

While issuers control the authentication stream, merchants control when to invoke EMV 3DS. There may be times where the issuer wants a stepped-up authentication, but because merchants have other information about the consumer, in some instances opting out could decrease false positives and create a better consumer experience.

4.2.6 Consumer Impact/Level of Friction

EMV 3DS has less consumer friction and cart abandonment than 3DS v1.0. Unlike 3DS v1.0, EMV 3DS automatically enrolls all consumers of participating issuers, so consumers do not need to explicitly enroll to use the service.

The risk level determines the need for a challenge, so not all CNP transactions require cardholder interaction. EMV 3DS allows more sophisticated authentication methods (e.g., biometrics, OOBA, tokenization for two-factor authentication), relying less on PII, static passwords and KBA to verify consumer authenticity if challenged.

4.2.7 Implementation Considerations

For a EMD 3DS transaction to occur, EMV 3DS must be implemented by both issuers and merchants. If either party does not support EMV 3DS, such a transaction cannot occur.

Implementation of 3DS domains depends on how the 3DS client communicates (e.g., directly with 3DS server, combined 3DS server and merchant server, or other). Issuers should engage with an ACS provider that has step-up authentication options and can explain how its models help maximize detection and minimize false declines.

Issuers must onboard card portfolios to the EMV 3DS platform and then test and certify with the card networks.

Merchants must also make sure they have the appropriate technical resources to make changes to their systems to prepare for EMV 3DS.

4.2.8 Maturity and Effectiveness of the Technique

3DS v1.0 was decommissioned in 2021 by Visa, and in 2022 by Mastercard.[118]

EMV 3DS replaced v1.0 in 2017 and provides improvements and enhancements. Multiple locations have implemented EMV 3DS, but implementations have not reached maturity.

Multiple processors, payment networks and other providers offer solutions that leverage EMV 3DS. Each major payment network has a proprietary EMV 3DS solution: Mastercard Identity Check, Visa Secure, Discover ProtectBuy 2.0, AmEx SafeKey.

Per Visa,[119] checkout time with EMV 3DS decreases by 85% and cart abandonment decreases by 70%. About 95% of the online merchant's transactions are deemed low risk, and pass without a challenge or interruption to the consumer checkout experience, depending on the merchant's confidence level.

4.2.9 Applicable Industry Standards

EMV 3DS is a global specification.[120]

4.2.10 Publicly Available Statistics on Implementations and Use

Statistics are not available for this technique.

[118] When Will 3D Secure v1 Be Discontinued?, PayZen

[119] TASgroup.eu. "The New 3D Secure 2.0. A Quick Guide." 2019

[120] EMV 3-D Secure-Protocol and Core Functions Specification v2.0.0, EMVCo.

4.3 Identification and Verification (ID&V) and Provisioning

4.3.1 Definition/Description

ID&V plays a key role in determining whether a consumer is the legitimate owner of the account credentials linked to a wallet before replacing the PAN with a payment token. If not performed effectively, ID&V is a critical point of vulnerability. The level or strength of the authentication method should match the risk being mitigated.[121]

Issuers perform ID&V as part of the provisioning process to ensure that the consumer is the legitimate owner of the payment credentials before the payment token is created and provisioned to a mobile wallet. **The process is not repeated for each transaction**. Examples of ID&V methods include an account verification message, PAN-based risk score assessment, and one-time password. The process, which assumes the KYC process has already occurred, can entail physical card possession and/or additional authentication methods, and allows for issuance of standalone digital cards without a physical card. Some issuers follow up with an email or letter to confirm the account provisioning.

There are two forms of token provisioning, card-on-file token provisioning and mobile wallet token provisioning (MWTP). This white paper focuses on MWTP. Three model scores are typically provided for MWTP, one by the network (the token provision score [TPS]), and two scores by the mobile wallet provider (device and account). The network-provided TPS ranks the risk based on device/account profiling of prior risk factors on the network involved. Similarly, the MWTP account and device scores rank the risks of the account and of the device separately.

4.3.2 Applicability

In the context of this paper ID&V is associated with provisioning a payment token by the issuer to the consumer's mobile/digital wallet during the enrollment process, sometimes in concert with the MNO or hardware manufacturer. Once provisioned, the token is used in lieu of the PAN when making in-app and mobile app purchases.

4.3.3 Technical Features

The token assurance method is set during token issuance and can be updated. EMV 3DS revised the former token assurance level concept to represent a consistent value related to token assurance that is based on: (1) type and outcome of the ID&V process during provisioning; (2) entity performing ID&V; (3) domain in which the payment token is to be used; and (4) supporting token assurance data. The values assigned focus on the facts of "what" ID&V method was done and "who" (typically the issuer) performed the ID&V method, and are used to assign a risk score to the token.[122]

[121] "Mobile and Digital Wallets: U.S. Landscape and Strategic Considerations for Merchants and Financial Institutions," U.S. Payments Forum, 2018

[122] EMV® Payment Tokenisation Specification – Technical Framework v2.3, EMVCo, 2021

4.3.4 How the Technique Works

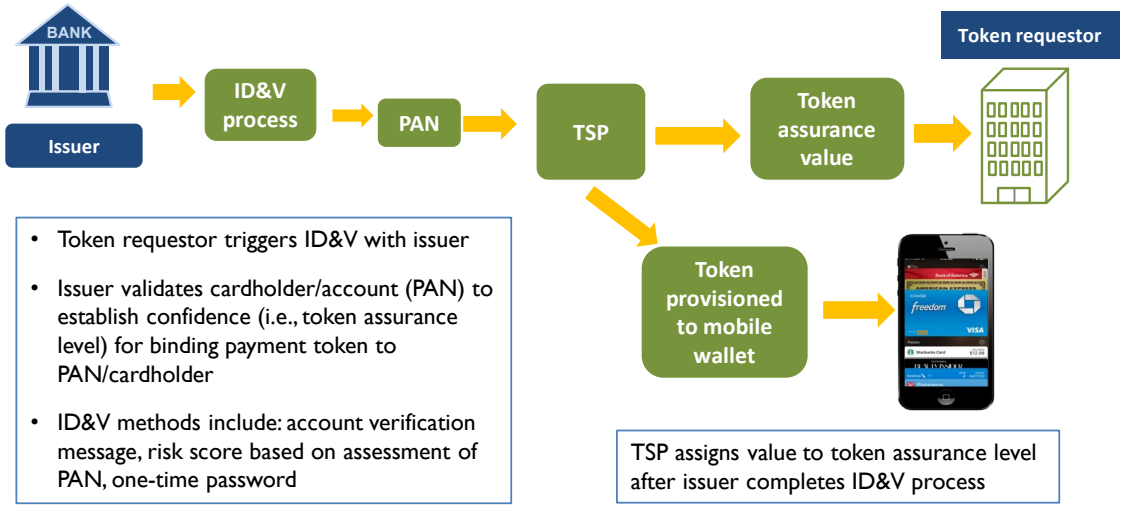

Figure 18. ID&V Provisioning[123]

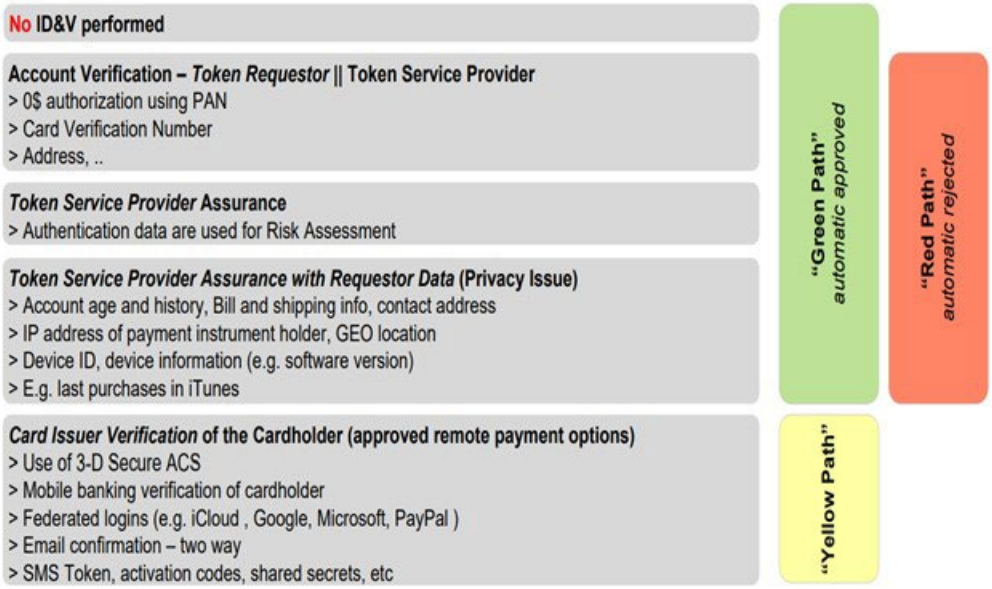

Figure 19. ID&V Methods[124]

[123] U.S. Payments Forum, "Mobile and Digital Wallet Webinar Series Part 2: Security Technologies & Approaches," Jan 2019.

[124] Apple Pay: How different is it from other Pay solutions, what role does tokenization play, and to what degree can CNP payment benefit from Apple Pay in the future? Semantic Scholar, 2018

4.3.5 Risks Associated with the Technique

If a fraudster obtains consumer enrollment data, the fraudster can use his/her own biometric data and stolen payment credentials to register the account with another online or wallet provider. Therefore, verifying the identity of the consumer is a first point of vulnerability. Unless the person has been verified as the legitimate owner of the account, it will not matter what other security methods are applied during the transaction process, because the fraudster will have control of the account.

When Apple Pay was introduced, there was initially a spate of fraudsters provisioning stolen credit cards into wallets to buy big-ticket items in Apple Stores and other retailers.[125] As a result, issuers adopted additional verification protocols such a one-time activation codes, challenge questions, or person-to-person verification by calling a consumer service representative and engaging the fraud team if needed.

4.3.6 Consumer Impact/Level of Friction

The degree of friction depends on the perceived riskiness of the account being provisioned. The higher the risk score, the more friction introduced, as with one-time activation codes, challenge questions, and requirements to call a consumer service representative.

4.3.7 Implementation Considerations

The ID&V process examines the risk assurance score and any additional data to decide whether to provision a payment token to a mobile wallet. For example, a mobile wallet provider may also review certain data elements (e.g., age of account, device ID, history of phone activity, phone model, geolocation), and generates and shares a risk score with the issuer to aid in the risk assessment. If the risk assessment determines that the account is low risk, the issuer can automatically accept it and provision the token to the mobile device.[126] The issuer has the final say on whether to add a card to the wallet.

The ecosystem gets significantly stronger model scores when issuers participate in device-level fraud reporting. Some wallet providers may accept bad devices from the issuers, and then send elevated risk flags in addition to the model scores for issuers to leverage in mitigating future risk. A key point is that all federally regulated issuers are required to have strong model risk management practices, and an inventory of all models in service for the bank. These models require testing and validation, and for vendor-provided fraud/risk models at minimum, regular validation through performance monitoring that the model performs accurately during adverse conditions of fraud attacks.[127]

4.3.8 Maturity and Effectiveness of Tool

ID&V is a mature tool, used prior to internet banking. With the launch of the NFC mobile wallets (e.g., Apple Pay, Google Pay and Samsung Pay) in 2014 the importance of performing ID&V increased.

Next generation ID&V techniques are trending toward increased use of biometrics and machine learning.[128]

4.3.9 Applicable Industry Standards

None noted.

---

[125] Banks reportedly clamp down on Apple Pay card provisioning in wake of fraud, Apple Insider, 2015

[126] "Adapting to Mobile Wallets: The Consumer Experience," Federal Reserve Bank of Boston, June 2017

[127] SR 11-7: Guidance on Model Risk Management, The Federal Reserve, April 2011.

[128] 5 Trends That Prove Digital Identity Verification is More Relevant Than Ever | OneSpan July 2020.

4.3.10 Publicly Available Statistics on Implementations and Use

Statistics are not available for this technique.

5. Analytics and Familiarity Signals

Familiarity (positive) signals provide a level of positive identity assurance, or through anomalies, risk, and attack (negative) signals for high risks. The relationship can be established through an active enrollment process, or be passive, contingent on a successful authentication with sufficiently high assurance levels. Data from predictive analytics and machine learning techniques help to determine the level of identity assurance.

5.1 Predictive Analytics

5.1.1 Definition/Description

Predictive analytics tries to determine 'what will happen' rather than 'what happened' or 'why did it happen.' It is the process of using analytics to make predictions based on data. This process uses data along with analysis, statistics, and machine-learning techniques to create a predictive model for forecasting future events, behaviors, or most likely outcomes (e.g., potential fraud occurrences). Large amounts of data-rich historical transaction details, along with supplemental data such as device intelligence and account details, are used to build a rules engine and score transactions using a risk-based approach. Iterative by nature, the predictive model can learn from new fraud activity and optimize accordingly, while enabling decision-making processes in real-time.

Predictive risk monitoring helps organizations discover potential risks and threats, including types of risks not covered by existing risk indicators. Risk monitoring applies analytics to current and historical information from internal and external data sources to identify emerging risks with a short cycle to impact. Such a capability helps modernize an established risk management framework from periodic risk reporting to real- and near-real-time risk reporting, known as predictive risk intelligence (PRi).

Types of data collected include:

- User behavior (browsing speed, pages visited)
- Transaction specifics (purchase cost/time/volume/method)
- Device specifics (device reputation, geolocation, language, compromised device [malware/jailbroken], device emulation)
- Suspected upcoming fraud behavior (e.g., from proactive dark web scraping)
- Past exposure of consumer data (e.g., from previous breaches)
- Use of link analysis[129] to identify hidden connections and relationships in a data set that are otherwise hard to spot. Common types of networks include:
  - Social networks that reveal who is speaking to whom
  - Semantic networks that reveal and highlight related topics
  - Conflict networks showing connections and alliances among entities

[129] Using large amounts of data (or big data) precludes filtering or analyzing data with traditional methods. Data used to predict fraud is also complex, continuously changing and varied. Link analysis is a technique used to assess and evaluate connections between data, and to investigate fraud in an interactive and intuitive way to identify patterns and trends and drastically reduce the time and effort required to expose fraud patterns. It is also called 'network visualization' because the data is shown in a graph network. See full article here.

5.1.2 Applicability

FIs, processors, payment networks and merchants may all use risk-based analytics. The technique is applicable primarily for the payment transaction process. Risk-based authentication (RBA) predictive analytics is payment-method agnostic and can be used for consumer verification or device authentication.

5.1.3 Technical Features

RBA predictive analytics develops static and self-learning predictive algorithms (data-driven statistical model) by combining analysis of internal and external precursor information. The model is used to predict or detect heightened occurrence and likelihood of risk event

Data mining and machine learning (ML)[130] capabilities allow models to be maintained and/or evolve with ongoing improvements to accuracy. This is most effective with automated ways to continue to feed the models new data as soon as it is available. A system with real-time responses is less effective if it is trained with old/stale/aging data.

RBA predictive analytics is hosted in the cloud and incorporates multiple data streams.

5.1.4 How the Technique Works

Predictive analytics applications incorporate three fundamental components:

- **Data**. The quality of the data available for processing is a key factor in the effectiveness of the predictive model. Reviewing (e.g., cleaning, ignoring, etc.) prior to inputting the data into the system to make decisions is critical.[131]
- **Statistical modeling**. Used to derive meaning, insight, and inference from the data. Predictive analytics uses various statistical techniques, with regression used the most.
- **Assumptions**. Predictive analytics draws conclusions from the collected and analyzed data that usually assume that the future will follow a pattern related to the past. Defining the past is an important exercise to determine what timeframe is generally the most predictive. Many models refer to the previous year to account for seasonal variances and smooth outliers in the data.

Predictive analytics interprets patterns from data, which are then extrapolated to make decisions. Predictive analytics uses these techniques for decisioning in real time. The amount of data available allows behavior to be checked from a multitude of angles. Because the model can identify legitimate consumer behavior, it allows for detection of anomalous or suspicious activity. It can also identify typical or suspected fraudulent behavior. The model can be updated frequently, allowing it to spot fraudulent patterns even in the nascent stages, and is able to provide robust output to fraud experts to understand what assessments are being made and why.

A predictive analytics model can identify potential trends and correlations. Examples include PRi-enabled analytics, chronology of events, external alerts, cross-database pattern recognition, and behavioral analytics.

[130] See Section 5.2 for a definition/description of machine learning (ML).

[131] A data audit might also be helpful to know what data is potentially available for the organization to use.

5.1.5 Risks Associated with the Technique

Predictive analytics is subject to predictive modeling errors. Biases could exist with the model, or the data used. If predictive analytics tries to model something that cannot be modeled using a 95% confidence interval, 5% of random occurrences could come up as statistically significant. Furthermore, statistics carry some risk of being wrong. The use of old, stale data or data that is not properly cleaned could lead to inaccurate results.

5.1.6 Consumer Impact/Level of Friction

This technique has minimal consumer friction.

5.1.7 Implementation Considerations

Implementers can purchase software and create their own predictions or use vendors to develop models and visualizations. Implementations may require multiple solution providers.

Collecting the data and building the model are complicated and time-consuming. The process requires specialized knowledge to figure out how to use the data and a lot of backend work to succeed.

Implementation is complex because it requires either a dedicated team of data scientists to parse the data sets, or a software suite powerful enough to do so rapidly. This may limit the ability of small and medium-sized businesses to realize its potential value.

Because modeling software is not knowledgeable about a specific industry, business, or niche group, it may require customization to meet their specific needs to be effective. For example, an issuer with high income customers might have a very different model than one for lower income customers.

Predictive analytics has high implementation and ongoing maintenance costs. Implementers may find it difficult to justify a return on investment (ROI).

Educating stakeholders on how to interpret the data is very important to ensure that everyone agrees on how to respond to what they are seeing in the data.

Other considerations include:

- The analysis is not always real-time.
- Implementation requires reliable and comprehensive risk and performance data.
- Effectiveness relies on data governance and integrity measures.
- The technique cannot replace a periodic risk assessment process.

RBA predictive analytics has the following characteristics:

- Captures comprehensive, holistic view of risks
- Predicts potential risks before they become threats
- Identifies and monitors emerging risks
- Recognizes emerging risk trends
- Automates analyses through cognitive intelligence and applied robotics
- Allows for prompt escalation and remediation through integrated risk analyses
- May be used to predict individual behavior in real time to enable a system to know when consumer behavior is out of character and evaluate risk
- Provides the ability to detect anomalies to flag unusual consumer behaviors and then react to prevent fraud

5.1.8 Maturity and Effectiveness of the Technique

Various payment processors and security vendors offer risk-based predictive analytics tools but may lack sufficient data on adoption. They also require highly skilled data scientists to develop models and interpret data. As a result, this technique is not mature, and usage is limited.

Smaller FIs and merchants may not be able to determine the ROI to justify the initial investment in a solution. Alternatively, they can work with third parties if they believe the investment is worthwhile.

The technique can be more effective if stakeholders leverage existing tools (e.g., MFA) and other access tools.

5.1.9 Applicable Industry Standards

To date, most of the focus around predictive analytics standards has been on the Predictive Model Markup Language (PMML) model interchange format. This format, developed by the Data Mining Group (DMG), an independent, vendor-led consortium, is well established in the analytics space. Most analytic tools support the export of PMML models, and a number of tools support the deployment of PMML models into production. The DMG is in the process of releasing a new standard to complement PMML. The standard, named Portable Format for Analytics (PFA), incorporates improvements informed from observing the use of PMML over many years.[132]

5.1.10 Publicly Available Statistics on Implementations and Use

Statistics are not available for this technique.

[132] Big Data https://dzone.com/big-data-analytics -tutorials -tools -news, https://dzone.com/big-data-analytics-tutorials-tools-news DZone, Dec. 2020 and Data Mining Group

5.2 Machine Learning/Artificial Intelligence for Authentication

5.2.1 Definition/Description[133]

Artificial intelligence (AI) is a collection of technologies that combine data, algorithms, and computing power to act like a computer with human intelligence. AI produces machines able to autonomously perform tasks that would normally require human intelligence by giving them the ability to perceive, learn from and act using data. It requires constant, good quality input data.

Machine learning (ML) is a subset of AI, with a key difference – 'learning.' Inputting large amounts of data to a computer trains ML how to make decisions about the data, similar to how a human would respond, but with the ability to act on patterns too complex for humans to identify.

ML has supervised and unsupervised components. It creates a risk score with context for each transaction and helps fraud reviewers gain deeper understanding of the transaction to enable them to approve more good orders or to recognize other fraudulent behavior.

ML assigns risk levels based on known risk factors, and identifies riskier transactions, which are subject to augmented intelligence. The risk engine increases the number of hurdles for would-be fraudsters, while streamlining the experience for good customers, helping to decrease online abandonment rates.

The ML model consists of multiple algorithms that combine all features (data characteristics) to produce a risk score. The model continually queries extracted features to make a fraud prediction and provide the best reaction in milliseconds. Different ML models are used for different cases – e.g., for email verification vs. payment types. Combining a variety of ML models provides more accurate results.

ML enables:

- Real-time decisions, based on risk scoring and decision-making in low latency[134]
- Parallel dataset processing, which allows analysis of more data while still maintaining real-time decisions without trade-offs between data and latency
- Reduced cycle time, continuous not batch, with transactions being scored also updating/teaching the ML models
- Increased effectiveness, enabling detection of very subtle patterns and variations
- Processing of enormous amounts of data

ML vs. Rules-based Systems for Fraud Detection

Many banking and ecommerce stakeholders use traditional fraud detection systems that are rules-based – i.e., the system assesses the risk of each transaction/individual account by applying a set of rules or conditions. The rules use algorithms that perform fraud detection scenarios. On average, legacy systems may apply about 300 different rules to approve a transaction. Typically, fraud prevention teams write the rules manually, and must constantly add or update rules to reflect new types of fraud. The process is straightforward, making the process difficult to detect implicit correlations.

---

[133] Ravelin Insights. "Machine learning for fraud detection." 2020

[134] Fraud has grown to epidemic proportions. Digital and mobile card payments have dramatically increased both transaction volumes and attack vectors for fraudulent activity, taxing payment processors to speed up their ability to take anti-fraud measures. The compound challenge is driven by the speed at which malicious acts can occur. This necessitates fraud detection algorithms that identify suspicious behaviors not in seconds or even milliseconds, but in microseconds. 39% of IT decision-makers in financial services named cybercrime prevention a top priority in their efforts to reduce latency. The faster the payment process, the more fraud detection algorithms can run in the available window of time –which has the potential to dramatically improve fraud prevention and save companies millions of dollars. BAI Banking Strategies, February 5, 2020.

With evolving ecommerce payment schemes and the desire for faster approvals and friction free checkout, fraudsters continue to find new ways to commit fraud. Organizations that use a rules-based approach cannot keep up.

Machine learning creates algorithms that process large datasets with many variables and helps find hidden correlations between user behavior and the likelihood of fraudulent actions. Machine learning is more effective for scenarios requiring a fast pace of change and that are not easy to translate to a list of set rules.

It also requires less manual work than rules-based approaches. For example, ML algorithms can work with behavior analytics to reduce the number of verification steps needed to approve a transaction.

5.2.2 Applicability

Machine learning applies to account creation/account takeover (ATO), provisioning/enrollment, transaction processing, consumer verification or device authentication. However, it is used primarily to identity fraudulent transactions.

5.2.3 Technical Features

Good fraud detection models use a combination of supervised and unsupervised ML and advanced anomaly detection to draw insights from data networks. (Figure 20.)

The supervised ML model is trained on historical activity and variables with known fraud and non-fraud cases to enable it to detect known or previously seen fraud attacks. The model looks for past fraud patterns and automatically identifies new instances of these fraud types in new data. It can analyze billions of historical transactions from a data network and look for signals that have predicted fraud in the past based on the historical variables.

The unsupervised model uses clustering (segmentation) to group similar entities (e.g., service providers, consumers). The model identifies anomalous or outlier behaviors that indicate a new type of fraud attack by using advanced algorithms and models to detect transaction anomalies much faster, more accurately, and on a more scalable basis than human judgment alone. It can find previously unknown or emerging types of fraud attacks that supervised ML cannot catch and find them before they result in fraud.

Both ML models must be trained with enormous amounts of data.

Both use technology to analyze safety patterns and weigh them against risk signals and anomalies to catch transactions that are high risk.

SUPERVISED LEARNING	**CLASSIFICATION** Algorithms to predict classes: • Fraud • No fraud	**REGRESSION** Algorithms to predict numbers: • Fraud risk scores • Expected values
UNSUPERVISED LEARNING	**GROUPING** Group similar items together: • Segmentation • Clustering • Item sets • Association rules • Sequence analysis • Network analysis	**ANOMALY DETECTION** Find outliers in your data • Unusual behaviors

Figure 20. Machine Learning: Feature Extraction and Selection[135]

5.2.4 How the Technique Works[136]

Building and using a ML model requires multiple steps.

1. Data is input, cleaned, and normalized.

   If the ML model is supervised, the data must be labelled as good (e.g., real consumers who have never committed fraud) or bad (e.g., consumers with chargebacks or manually labelled as fraudsters).

2. Extraction transforms the raw data into structured, machine-processable formats that the ML algorithm can understand (labelling). Extract features may include data to describe good consumer behavior and fraudulent behaviors (known as fraud signals). Feature types include:
   - Identity (email address, account age, number of devices, and fraud rate of consumer IP address)
   - Orders (number made, failed, average order value, risky basket contents)
   - Payment method (fraud rate of issuing bank, similarity between consumer and billing name, cards from different countries)
   - Locations (shipping vs. billing address, shipping country vs. consumer IP address, fraud rate at consumer location)
   - Network (number of emails, phone numbers or payment methods shared within network, age of consumer's network)

[135] 'Machine Learning for Fraud Detection' presentation. RapidMiner, October 2018.

[136] Ravelin Insights. "Machine learning for fraud detection." 2020

3. The algorithm is trained using rules and the features above to learn how to make fraud predictions.
4. The model is built and deployed based on training the algorithm.
5. Fraud teams feed the model with data, analyze transactions and re-input the outcome data, as well as look for other trends the model may not have identified. This step can introduce bias.
6. Multiple models can be applied to the same transaction.
7. Once the model is operational, it is evaluated and monitored. An iterative process is used to regularly improve and update the model to detect the latest fraud techniques.

Figure 21. Machine Learning Flow[137]

Machine learning relies on good quality input data to avoid making erroneous fraud assessments. It is only as good as the people who evaluate the data to determine the level of fraud. Combining ML with rules-based systems adds value because the rules complement ML and can serve as a set of guidelines that give businesses more immediate controls over fraud decisions. Machine learning should be combined with additional processes to determine next steps on a high-risk score.

5.2.5 Risks Associated with the Technique

There are several risks associated with ML.

- Implementation and use are very complex and have a steep learning curve. Data science knowledge and amount of time and data needed to create models are challenging.
- It is difficult to keep models current with constant business changes.
- A machine lacks common sense, so it needs skilled humans to supervise and identify irrelevant data and results.
- Unintentional bias from human input could occur if solutions are not monitored.
- Machine learning is not good at dealing with uncertainty, so those types of cases need more human insight.
- Machine learning is not a silver bullet. Performance can vary between algorithms. It should be tailored to specific needs and events and use a comprehensive approach with multiple models to find the best combination of predictors for each customer, in each vertical, and for each type of fraud it is trying to prevent.

[137] Cybersource. "Machine Learning: a silver bullet? Role of machine learning in fraud management." 2019.

5.2.6 Consumer Impact/Level of Friction

Incorporating ML into a risk assessment does not directly impact the consumer. When a risk threshold is breached, other processes may be invoked and could result in further scrutiny, e.g., step-up authentication. The goal of ML is to prevent fraud by stopping bad transactions, while allowing good transactions to be processed.

5.2.7 Implementation Considerations

ML may be invoked by an issuer, a processor, a payment network, or a merchant. Each party could have a proprietary ML model that relies on its own data, and possibly third-party data to feed the model. Vendor models may combine data from multiple parties for better analysis but would not share individual data with other parties. Stakeholders could share specific data points and/or risk scores with other parties to the account or transaction (e.g., when determining whether to invoke EMV 3DS).

Implementation challenges include:

- Cost, complexity, and transparency of information associated with such solutions. The investment in technology and specialized human resources is a significant barrier to entry.
- The scarcity of individuals with fraud-specific domain expertise along with ML expertise limits the ability of many organizations to effectively use ML.
- Data sourcing, cleaning, and aggregation are challenges.

The following are considerations for implementing ML:

- Understanding and acquiring the level of internal domain expertise required to administer an ML solution.
- Understanding how a solution interprets the ML process into meaningful business intelligence, such as data discovery or explainable outcomes.
- Determining what data signals are needed and available within the detection system to develop and deploy effective ML-based detection strategies.
- Understanding why the model is making certain decisions. The ML model has hundreds of variables and needs the capability to capture interactions between and among multiple variables, which is difficult.
- Determining the right risk threshold. Implementation is a balancing act between true positives (i.e., the number of fraudsters blocked), false positives (i.e., the number of good consumers blocked), and false negatives (i.e., the number of fraudsters allowed). This level varies by business based on transactions (e.g., high or low volume, high or low value).

AI/ML implementation best practices include:

- Implementing a layered approach to protect different consumer interaction points in the payment stream, including authentication and consumer-initiated events.
- Using large volumes of data to ensure statistical significance.
- Labeling data to train the machine to achieve more accurate results.
- Determining whether to buy vs. build a solution. This decision depends on the size and type of business. Anecdotally, smaller ecommerce merchants with little data are more likely to use a third-party solution through their ecommerce platform processor. This type of solution has scale and a lot of data to build a generic model based on historical fraud patterns and use common algorithms across clients.

5.2.8 Benefits

Artificial Intelligence and machine learning offer multiple benefits for mitigating fraud.

- ML solutions are proactive. They report what is happening and learn across many data elements. ML assesses individual consumer behavior as it happens by constantly analyzing normal consumer activity; when it spots an anomaly, ML can automatically block or flag a payment for analyst review.
- An ML solution learns from patterns of normal behavior. It can adapt quickly to changes in that normal behavior and identify patterns of fraud transactions.
- ML can prevent fraud without impeding user experience and decrease false positives through sophisticated behavioral analysis.
- ML systems are scalable and improve with larger data sets. More examples of good and bad (i.e., real vs. fraudulent) consumers help identify differences and similarities between behaviors more quickly to predict fraud in future transactions. (In contrast, rules-based systems must expand to add increasing amounts of payment and consumer data.) Because ML is more accurate at scale, it may also uncover non-intuitive patterns or subtle trends not immediately obvious to a human.
- ML is more efficient and less costly than hiring and managing many fraud analysts to analyze hundreds of thousands of payments, which ML can do in seconds and produce results in real-time (milliseconds). Machines can perform repetitive, tedious tasks 24/7 and only escalate decisions to humans on an exception basis, when specific insight is needed.
- Implementing ML may reduce the size of fraud team and need for manual review with fast interacting machine models.
- Using ML does not replace the fraud team but gives them the ability to reduce the time spent on manual reviews and analysis. Analysts can focus on the most urgent cases, assess alerts faster with more accuracy, and reduce the number of genuine consumers declined.

5.2.9 Maturity and Effectiveness of Tool

AI/ML has come a long way and is making an impact in financial services; however, it is still considered in the early stages of development.

Many available solutions exist in the market, but are costly and may not be cost-effective or well understood by various industry segments

More computing power and distributed computing technologies allow data scientists and developers to expand the complexity and types of algorithms that build ML models, reducing the time it takes to analyze, build, and deploy models. ML continues to evolve as it incorporates more advanced techniques and additional data.

5.2.10 Applicable Industry Standards

- NIST, Artificial Intelligence[138]
- https://www.iso.org/standard/80655.html?browse=tc (under development)
- CFA Institute, Machine Learning[139]

[138] Artificial Intelligence, NIST,
[139] Machine Learning, CFA Institute, 2022

5.2.11 Publicly Available Statistics on Implementations and Use

Altexsoft reported the following statistics:[140]

- According to Feedzai, a well-trained ML solution can identify and prevent up to 95% of all fraud and minimize cost of manual reconciliations, which represent about 25% of fraud expenditures.
- According to Capgemini, fraud detection systems using ML and analytics minimize fraud investigation time by 70% and improve detection accuracy by 90%.

5.3 Device Familiarity, Risk and Attack Signals

5.3.1 Definition/Description

Detection of familiarity, risk and attack signals is generally passive. These signals are attributes or events originating from a mobile device that can be used to assess the security of an authentication session. These signals can be leveraged to add contextual information for user authentication by providing additional assurance that the authenticating user is valid. For example, in situations where user credentials may have been compromised, device signals can be compared against what is expected for a particular user's device. Mobile device signals are inherently digital, and can serve as passive, secondary authentication factors, in conjunction with a primary authentication mechanism, to make enhanced authentication decisions without explicit intervention from the consumer. These types of signals are typically put into three categories:

- ***Familiarity signals*** are affirmative signals issued to a device, or passive attributes that are gleaned from existing data flows (e.g., HTTP_ACCEPT headers). Using familiarity signals requires first establishing a relationship with the consumer. The relationship can be established through an active enrollment process, or be passive, contingent on a successful authentication with sufficiently high assurance levels. Examples of familiarity signals include, but are not limited to, browser cookies, digital certificates, biometrics, and geo-location.
- ***Risk signals*** are negative signals that indicate a potential risk with the mobile device, connection, or session. These signals are entirely passive in nature. Examples include transaction velocity, mobile device security posture, newly enrolled devices, use of anonymizing services, and geo-location (mismatch).
- ***Attack signals*** are negative signals that are typical of known attack patterns and behavior; and are entirely passive in nature. An attack signal may originate as a risk signal and be reclassified as an attack signal after evaluation. Examples of attack signals include detected attribute spoofing, non-human behaviors (bot detected), probing and penetration activities, and correlation of known fraudulent activity from other channels or past activity.

5.3.2 Applicability

Familiarity, risk, and attack signals can be leveraged to enhance authentication of mobile browser ecommerce, mobile in-app transactions, and provisioning payment cards to mobile wallets. While attack signal detection can provide standalone authentication decisioning data, risk and familiarity signals typically are combined and input to an RBA engine to determine the appropriate authentication mechanism required for a desired level of assurance.

[140] "Fraud detection: how ML systems help reveal scams in Fintech, healthcare, and ecommerce," ViitorCloud, 2021.

5.3.3 Technical Features

All signal categories rely on sampling a digital attribute or event. The sampling mechanism depends on the origin of the attribute or event and the digital channel. Generally, sampling of these attributes can be done in a mobile application (e.g., through a Software Development Kit [SDK] or a library) or in a browser session (e.g., Javascript collectors), depending on the use case. For example, a mobile banking application may collect the device's IP address.

This data is typically passed to a back-end server for analysis. The signals can be analyzed as part of a set of logical rules ("if then else" statements) or a more advanced risk-based authentication engine. The result of the analysis is incorporated into the authentication decisioning process and may affect that amount of friction introduced in the authentication session.

5.3.4 How the Technique Works

When a transaction requires authentication, the signals can augment the decisioning process and provide a level of assurance. If the assurance and confidence levels are sufficiently high, additional authentication may not be required. Conversely, if the assurance and confidence levels are too low, the transaction may be denied or require step-up authentication.

The party interacting with the consumer device (e.g., issuer, merchant) analyzes the signals to determine assurance levels, and may require analysis for the raw data to be useful. For example:

- Familiarity signals should be validated to ensure:
  - The signal has not been tampered with or spoofed (e.g., masquerading as a known user device/browser).
  - The signal matches the expected signal within a desired tolerance.
- Risk signals and attack signals should be evaluated to:
  - Determine the severity of the signal (e.g., how critical is this signal compared to others).
  - Assess the nature of the risk (e.g., is this a low-value transaction).
- Attack signals are evaluated to:
  - Determine the type of attack.
  - Reduce false positives and negatives.

5.3.5 Risks Associated with the Technique

An inherent risk of signal analysis is the quality of the signal and the assignment of the appropriate severity weight. Familiarity signals must be checked for validity to ensure no spoofing or tampering has occurred. Risk signals must be verified as accurate (e.g., not a faulty GPS transponder); and attack signals must be categorized properly (e.g., multiple failed login attempts could just be a user who forgot their password and not a bad actor mounting a brute-force attack).

Another risk is improperly utilizing the signals for authentication. As these signals help make authentication decisions, improper decisioning logic will render the technique ineffective. This would result in either a false decline or false acceptance, both introducing more friction into a transaction, declining a transaction, or allowing a fraudulent transaction.

5.3.6 Consumer Impact/Level of Friction

Due to the generally passive nature of signal detection, there is little to no impact to the consumer and no additional friction is introduced solely due to the signals. If being used in conjunction with RBA, additional friction may occur if attack signals are detected, or if they result in step-up authentication.

Consideration should be made for the privacy of consumer data and regulatory compliance. Signals such as geo-location information, IP addresses, and additional identifying attributes may be classified as PII and subject to legal fines and penalties if the appropriate controls are not implemented.

5.3.7 Implementation Considerations

A mobile application will use the device's native sensors to passively collect data on familiarity, risk, and attack signals and pass it to a back-end system, where the data is interpreted into signals. This can be done with native operating system APIs and functions or supplemented with a third-party SDK for quicker deployment and enhanced signal analysis.

A mobile browser session will use code on the web page to collect information and pass it to a back-end system, where the data is interpreted into signals. The technique is typically implemented with JavaScript or a similar scripting language to collect, parse, and pass the information to the back-end system for analysis.

Once the signals have been analyzed, the primary authentication system will use the results to make an authentication decision (e.g., allow, deny, step-up required).

5.3.8 Maturity and Effectiveness of Tool

The collection of digital signals classified into familiarity, risk, and attack have been used since the early days of ecommerce. The ability for a user with a "trusted endpoint" that can be identified using these signals has existed since at least 2003.

Due to the passive nature of these signals, they are highly effective at keeping consumer friction low, while providing additional assurance data. However, the signals are not effective as a standalone solution and require a primary authentication system to function.

When properly utilized, the signals can reduce the amount of customer friction, while simultaneously increasing the security of a transaction and decreasing fraud rates. The technique may be most effective when used with an RBA engine.

5.3.9 Applicable Industry Standards

Industry standards are not available.

5.3.10 Publicly Available Statistics on Implementations and Use

Statistics are not available for this technique.

6. Summary and Conclusions

As payment network requirements grow ever more complex and cybercriminals grow increasingly savvy, industry payment stakeholders need a well-designed, fully supported program to ensure compliance and to mitigate their risk. At the same time, security and fraud departments must continue to create new techniques to counter the more complex attacks.

This white paper was created by the members of the U.S. Payments Forum Mobile and Contactless Payments Working Committee to deliver a compilation of the techniques and tools used in reducing or eliminating mobile-initiated ecommerce/CNP fraud. As card-present fraud has decreased with the migration to EMV, fraud has migrated to the CNP channels. Different sources offer information on many of the fraud techniques included in this white paper. However, the industry has not had a coordinated and organized document that can be used as a **first** reference. This white paper provides that and a primer on the types of techniques that are available, their high-level functions, and some of the similarities and differences among techniques, so that payments stakeholders can ask informed questions of solution providers.

Many of the techniques used to mitigate mobile CNP fraud are recent developments and are difficult to explain in a short format. This paper provides a standard set of topics to help describe each technique and relevant information in a common format. The techniques described provide different means of addressing security for mobile CNP transactions, each delivering value for the conditions for which it was designed.

The techniques were grouped into four main categories for simpler navigation and to indicate which techniques were related. For mobile CNP security, no one solution works in all situations. A layered approach is needed to combat different types of CNP fraud. In general, more recently developed “risk-based” authentication techniques have become mature and are being adopted in more situations to combat mobile CNP fraud.

This white paper should be considered as a high-level guide of known current authentication techniques for mobile and in-app payments that are being used to combat mobile CNP fraud.

7. Legal Notice

This document is provided solely as a convenience to its readers. While great effort has been made to ensure that the information provided in this document is accurate and current, this document does not constitute legal or technical advice, should not be relied upon for any legal or technical purpose, and all warranties of any kind, whether express or implied, relating to this document, the information or materials set forth or otherwise referenced herein, or the use thereof are expressly disclaimed, including but not limited to all warranties as to the accuracy, completeness or adequacy of such information or materials, all implied warranties of merchantability and fitness for a particular purpose, and all warranties regarding title or non-infringement. All third-party materials referenced herein are the property of their respective owners, the U.S. Payments Forum is not responsible or liable for the content or use thereof, and all references to or summaries of such third party materials are qualified by the actual third party materials, as made available by such third parties. Stakeholders interested in CNP fraud mitigation techniques are strongly encouraged to consult with their respective payment networks, acquirer processors, and appropriate professional and legal advisors regarding all aspects of security and implementation, prior to any implementation decisions.

APPENDIX

Acronyms

2FA	Two-Factor Authentication
3DS	3-Domain Secure
AA	Adaptive Authentication
AAMVA	American Association of Motor Vehicle Administrators
ACH	Automated Clearing House
ACS	Access Control Server
AI	Artificial Intelligence
API	Application Programming Interface
ATO	Account Take over
BLE	Bluetooth Low Energy
CA	Certificate Authority
CDCVM	Consumer Device Cardholder Verification Method
CDMA	Code Division Multiple Access
CNP	Card Not Present
CoF	Card on File
CRAM	Challenge-Response Authentication Mechanism
CTAP	Client-to-Authenticator Protocols
CVM	Cardholder Verification Method
DCF	Digital Card Facilitator
DDA	Demand Deposit Account
DMG	Data Mining Group
DPA	Digital Payment Application
DS	Directory Server
DSS	Data Security Standards
EFT	Electronic Funds Transfer
ERR	Equal Error Rate
EU	European Union
FAR	False Accept Ratio
FFIEC	Federal Financial Institutions Examination Council
FIDO	Fast IDentity Online
FI	Financial Institution
FRR	False Reject Ratio
GDPR	General Data Protection Regulation
GSM	Global System for Mobile Communication
GSMA	Global System for Mobile Communication Association
HE	Header Enrichment
HMAC	Hashed Message Authentication Code
HOTP	HMAC-based One-time Password
HSM	Hardware Security Module
HTTP	Hyper Text Transfer protocol

IBIA	International Biometrics Identity Association
ICAO	International Civil Aviation Organization
ID&V	Identity and Verification
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IMSI	International Mobile Subscriber Identity
IOT	Internet of Things
IP	Internet Protocol
ISMG	Information Security Media Group
ISO	International Organization for Standardization
IVR	Interactive Voice Response
KBA	Knowledge-Based Authentication
KYC	Know Your Customer
MFA	Multi-Factor Authentication
ML	Machine Learning
MNO	Mobile Network Operator
MO	Mobile Originated
MWTP	Mobile Wallet Token Provisioning
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
ODCVM	On-Device Cardholder Verification Method
OOBA	Out-of-band authentication
OS	Operating System
OTP	One-Time Passcode
PAN	Primary Account Number
PCI	Payment Card Industry
PFA	Portable Format for Analytics
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PMML	Predictive Model Markup Language
POS	Point of Sale
PRi	Predictive Risk intelligence
PSP	Payment Service Provider
RBA	Risk-Based Authentication
ROI	Return on Investment
SDK	Software Development Kit
SIM	Subscriber Identification Module
SMS	Short Message Service
SRC	Secure Remote Commerce
SRC PI	Secure Remote Commerce Participating Issuer
SRCI	Secure Remote Commerce Initiator
SSL	Secure Socket Layer

TEE	Trusted Execution Environment
TLS	Transport Layer Security
TOTP	Time-based One-Time Password
TSP	Token Service Provider
U2F	Universal Second Factor
UAF	Universal Authentication Framework
W3C	World Wide Web Consortium