# CONTENTS

GLOBAL PAYMENT AUTHENTICATION STANDARDS ........................................... 2
WHY THERE IS A NEED FOR THESE STANDARDS .................................. 3
USAGE OF PAYMENT AUTHENTICATION STANDARDS .......................... 4
3D Secure (Worldwide) ........................................................................... 4
3D Secure 2.0 (Worldwide) ................................................................. 6
PaySecure (India) ................................................................................. 8
UnionPay Online Payments (UPOP) (China) ..................................... 9
MIR (Russia) ....................................................................................... 10
Asia Pacific ......................................................................................... 11
PSD2 Directive (Europe) ...................................................................... 12
CONCLUDING THOUGHTS .................................................................. 13
The fight to prevent fraudulent transactions in the eCommerce environment has been going on for over 20 years. Visa and Mastercard were the first to recognise the need to authenticate the cardholder during card-not-present eCommerce transactions, and so began the quest to develop a common payment authentication standard. However, as payment authentication standards evolve and new standards are developed by the various industry parties with a vested interest in reducing fraud, this quest has not been accomplished. Initially developed to provide cardholders confidence using their cards for online payments, the payment authentication standards are advancing to enhance and streamline the cardholder experience and provide additional security. Such advancements include payments via mobile apps and digital wallets, and providing alternative authentication options, such as biometric authentication. Card issuers are taking the onus off the cardholder by making risk-based authentication decisions based on additional information captured from the cardholder during the checkout process.

Payment authentication standards operate by providing an additional layer of protection, in the form of an authentication step during the checkout process. With standards developed prior to 2016, this step involves the payer being diverted from the payment process to a dialog with the card issuer, which requests unique authentication data associated with the account in use, such as a static or one-time password (OTP). Once the payer has been verified as the owner of the account and directed back to the payment process, the transaction can be completed.

Benefits of adopting payment authentication standards

1. Enhances security of online payment systems through identification of the payer
2. Improves trust between the merchant and the customer thereby reducing abandonment rates
3. Reduces fraudulent chargebacks, in particular ‘friendly fraud’, which accounts for 71% of all fraudulent chargebacks.

---

1 GPayments, “An Introduction to Authentication: The solution to online credit card fraud”: https://www.gpayments.com/Portals/0/pdfs/GPayments_Introduction_to_Authentication_Whitepaper.pdf
The standards governing payment authentication have been developed by the card brands, financial institutions, EMVCo, the National Payments Corporation of India (NPCI), the National Payment Card System (NSPK) of Russia, and the European Commission. EMVCo is a six member consortium comprised of American Express, Discover, JCB, Mastercard, UnionPay and Visa. EMVCo facilitates worldwide interoperability and acceptance of secure payment transactions within the payment industry. It also manages EMV, a technical standard for smart payment cards, introduced in 1994 by EuroPay, Mastercard, and Visa, with the goal of reducing physical card fraud. In 2001, Visa launched its 3D Secure payment authentication standard for card-not-present eCommerce payments.

Although 3D Secure was owned by Visa, it was created in open consultation with the payments industry and was subsequently revised and enhanced over the years, culminating in version 1.0.2 (3DS 1.0.2) and adopted by many of the global card schemes. In recent years, EMVCo has facilitated the development of a new version of the 3D Secure standard, version 2.0. The specification for 3DS 2.0 was published in October 2016 with the expected mandate for all payment transactions and authentication to be compliant by December 2020. Meanwhile, other in-country processing standards from various regions of the world, including China, India, and Russia, have entered the industry introducing UnionPay, PaySecure, and MIR, respectively.

### WHY THERE IS A NEED FOR THESE STANDARDS

eCommerce around the globe is expected to be in the region of US$2.4 trillion by 2019, with credit cards being the most popular method of payment. With the projected increase in online spending, an increase in fraud is also expected. Juniper Research, in a recent report, found that online transaction fraud is likely to increase to US$25 billion by 2020. This poses a big problem for the payment industry and one which needs to be addressed by enforcing security at the point of payment. Payment authentication standards are designed for online payments, to prevent fraudulent transactions by adding a layer of security to authenticate the cardholder during the process of payment authorisation.

This added security allows customers to pay with confidence, aimed to have a positive effect on transaction abandonment rates, which were found to be over 74% in Q1 2016 across 500 leading global brands.

---

3D Secure (Worldwide)

3D Secure, or 3 Domain Secure, is so named because of the three domains involved in payment transactions. The domains are the Issuer domain of the card issuing bank, the Interoperability domain of the card scheme’s infrastructure and the Acquirer domain of the merchants and banks to which payment is being made.

The first version of 3D Secure was originally developed by Visa in 2001 and branded as 'Verified by Visa'. It was extended to include mobile authentication of payments in 2005. Mastercard initiated its own standard, ‘Secure Payment Application’ (SPA) but later abandoned it and adopted the 3D Secure standard instead, branding it as ‘MasterCard SecureCode’. Subsequently, the 3D Secure standard was also adopted and branded by American Express as ‘SafeKey’, JCB as ‘J/Secure’, and Diners Club International/Discover as ‘ProtectBuy’.

3D Secure is based on the communication of XML messages across a secured channel, using the Internet Security Protocol, SSL/TLS. To use a 3D Secure service, the cardholder has to enrol for the service, by associating an authentication value, such as a password, with their payment card. The merchant also has to implement the use of 3D Secure within its site, by installing a Merchant Plug-in (MPI). The MPI communicates with the card issuer to see if the card is enrolled in the 3D Secure service. If it is, a response is sent back to the merchant, and a window is presented on the screen to the payer within the eCommerce site, where the payer will be authenticated using a password. If the password is correct, and the transaction is approved, the payment will be made and the transaction will be completed.

One of the main selling points of 3D Secure 1.0.2 is that it offers the merchant full liability shift against fraudulent transactions. If a user has to pass through another layer of authentication to authorise a transaction, it is less likely that the card is being used in a fraudulent manner.

---

Although 3D Secure is used throughout the world, it has better uptake in some countries than others. In 2014, Ingenico released the result of a study into 3D Secure usage across a number of European countries. The following results from the study show the usage in Europe, for example, is highly varied:

- Belgium: 81.8%
- Switzerland: 74.6%
- Netherlands: 60.1%
- United Kingdom: 52.5%
- Germany: 28%
- Spain: 16.6%

The high volume of successfully authenticated transactions within these countries varies from 95% upwards to 98% and above, indicating a robust authentication standard.

From a marketing perspective, transaction conversion rates, which are the percentage of website users that accept 3D Secure authentication when presented with it during a transaction, have been negatively impacted. This is due to the higher likelihood of transaction abandonment by the cardholder when faced with the additional authentication step.

The level of impact varies greatly among different countries. A report, by Adyen, exploring conversion rates for merchants implementing 3D Secure for all transactions, found that in the UK conversion rates uplifted by around 2.5%, whereas in China and the US, 3D Secure negatively impacted conversion rates by an average of 43%. It is expected that uptake for 3D Secure in those countries will increase with the release of 3D Secure version 2.0, due to its frictionless nature resulting from the prediction that most authentication activity will be invisible to the cardholder.

---

8 Ingenico, "3D Secure Landscape in Europe": https://payment-services.ingenico.com/~/media/files/panorama_3-d_secure_2014_en.ashx

Initially, online payments were PC desktop and browser based, but now they can also be made using mobile apps and sites, available on Android, iOS and Windows devices. The specification of 3D Secure 2.0 has been built to provide support for mobile payments, integration with browsers and mobile apps, risk-based security, multi-factor authentication, and digital wallets.

The 3DS 2.0 authentication process is also complemented by the use of tokens, which are one-time use credit card numbers. Although not an official part of the standard, they provide increased protection for cardholders against counterfeits, account misuse and other forms of fraud.

One of the key advantages of 3DS 2.0 is the enablement of authentication on a wider set of devices including mobiles, smart TVs, smart watches and gaming consoles. This enables authentication that is app-based, if the transaction is initiated on a mobile device within an app provided by the merchant; browser-based, if the transaction is initiated on a website; or console-based, for game consoles, which are not browser or app-based. In this way, authentication is possible on virtually any connected device from which purchases can be made. This device agnostic approach allows merchants to offer an extended sales platform, ensuring a more secure purchasing process across connected devices and channels.

To facilitate risk-based authentication by the issuer, 3DS 2.0 captures a varying amount of payer and device information, depending upon market or regional mandates to restrict sending of this information (such as device ID, MAC address, SIM card details, etc.), known as ‘rich data’. The information collected, including cardholder and transaction details, is encrypted and sent to the card scheme’s directory server where the data is decrypted, validated and then passed on to the card issuer (ACS). Based on this rich data, the issuer conducts a risk assessment in order to make a decision as to whether the person performing the online transaction is authorised to use the payment card.
Although cardholders may appreciate this faster and frictionless checkout process, a question arises as to whether those who are more conscious and protective of their personal data will have concerns as to what information is being held about them, exactly who has access to it and what other purposes that data may be used for.

The need to have open interoperable global standards does not appear to be addressed by the 3DS 2.0 standard. Further fragmentation of the payment authentication arena is likely as its specification not only lacks support for coexistence with 3DS 1.0.2 but also for other in-country standards that have been developed by countries such as India and Russia to support the processing of their domestic online payments. Additionally, whereas 3DS 1.0.2 was owned by Visa and created in open consultation with interested parties involved in the payment industry, 3DS 2.0 was created under the auspices of EMVCo. Contributors to the design of the standard include representatives from the EMVCo collective, together with those who are prepared to accept the US$25,000 annual fee for being EMVCo technical associates. This has greatly reduced the opportunity for other parties, such as consumer protection organisations and regulators, to provide constructive input before 3DS 2.0 solutions are implemented. These actions have effectively commercialised and productised the standard as evidenced by the ruling issued by the Australian Competition and Consumer Commission denying the Australian Payments Clearing Association’s request to mandate an industry wide security initiative using 3D Secure security measures because “mandating this one product into the market with no controls over access or pricing for payment schemes will harm competition and increase costs for Australian businesses and consumers” and “… if fraud rates for online card transactions continue to increase, it will be more attractive for businesses to take up security measures. Such measures might be 3D Secure or other existing or new products. These market forces can be expected to check the growth in online transaction fraud, without forcing businesses to adopt a particular product.”

Implementation of 3D Secure 2.0 is being supported through the EMVCo community and in collaboration with the PCI Security Standards Council (PCI SSC), who will be using the new specification as part of its information security requirements framework. According to a joint press release by EMVCo and PCI SSC, 29 September 2016, PCI SSC will provide security requirements, testing procedures, assessor training and reporting templates to address the environmental security associated with 3DS 2.0 and intend to release the related documentation in the first half of 2017.

As to when 3DS 2.0 will become available, deadlines for introducing and moving to support 3DS 2.0 compliance for all transactions vary depending upon the card scheme. Visa has announced that it is proposing a deadline for card issuers and merchants to migrate to version 3DS version 2.0 between April and October 2018, across the globe. Mastercard has shared its expected deadline of December 2020.

---


PaySecure (India)

India’s online transactions accounted for 14% of its total transactions in 2014, which are anticipated to increase as more people take up the use of smartphones.14 eCommerce in India is expected to be worth US$100 billion by 2020.15 Since these numbers were predicted, the November 2016 directive, by Prime Minister Modi, that all large denomination rupee notes should be eliminated from circulation and could only be exchanged for new notes by depositing them in a bank account, will have caused a marked growth in the number of new bank accounts, and hence bank cards, in the 85% of the total population of over 1.3 billion people that have never held a bank account before.16

To manage India’s domestic online transactions, the National Payments Corporation of India (NPCI), a not-for-profit organisation, has developed a card payment framework, which has been branded as RuPay. In a similar manner to the 3D Secure standard, RuPay has extended security through the use of payment authentication at the point of an online payment. The authentication standard used by the RuPay system is known as PaySecure.

As the Reserve Bank of India (RBI) has enforced the use of two-factor authentication for online transactions, most of the large banks in India are using PaySecure for the protection of online transactions, including ICICI Bank, State Bank of India, Bank of India, Union Bank of India, and Indian Overseas Bank.

The PaySecure authentication measures are set up during card registration for the service and are rules based with the rules setting the level of authentication required. For online transactions under a certain value, the payer will be required to authenticate using the two-factor authentication method, in the form of an image and a passphrase, followed by the card’s PIN. For transactions over a certain limit, prior to entering the card’s PIN, cardholders will be required to enter a one-time password (OTP) that has been sent to their registered mobile number, email address or device. An anti-phishing mechanism is also available, allowing the user to check their last three online purchases during the transaction.

NPCi, as a business and technical associate of EMVCo, is able to participate in EMVCo working groups for the creation, development, promotion and implementation of international standards, including the design and development of the 3D Secure 2.0 protocol.

---

14 Dazeinfo, "Online Payment In India Accounted For 14% Of Total Transaction Amount In FY 2015": https://dazeinfo.com/2015/05/29/online-payment-india-accounted-14-total-transaction-amount-fy-2015-report/
15 The Economic Times, "India’s ecommerce market to breach $100 billion mark by FY20": http://economictimes.indiatimes.com/articleshow/49532128.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
16 Financial Times, "India’s Modi seeks bank accounts for 75m poor households": https://www.ft.com/content/1195110e-2dd1-11e4-8346-00144feabdc0
UnionPay Online Payments (UPOP) (China)

By 2014, online transactions in China had increased year on year to 2.9 trillion Yuan (approximately US$419 billion). They are expected to reach 10 trillion Yuan ($1.45 trillion USD) by 2020. The UnionPay Online Payment Program (UPOP) is UnionPay’s eCommerce solution used by over 50 Chinese financial institutions to process online transactions. It works with 3.2 billion payment cards, more than Visa and Mastercard combined. UnionPay cards are also accepted across 150 countries outside of China.

UnionPay provides two cardholder authentication systems for the domestic market, SecurePay and ExpressPay. When payers are registered for SecurePay, they are redirected to the issuing bank’s site to authenticate themselves using the OTP sent to their mobile number. ExpressPay authentication is performed at the merchant site and also involves the use of an OTP sent to the payer’s mobile number. For the international market, UnionPay cards operate in the same way as standard cards in the payment systems of their co-brands.

UnionPay joined forces with EMVCo, in 2013, to contribute to their ongoing goal to create a universally consistent and secure infrastructure to support contact, contactless and mobile chip-based payments into the future and the design and development of the 3D Secure 2.0 protocol.

MIR (Russia)

The MIR (meaning ‘Peace’ or ‘World’) payment system is Russia’s national payment system.

The MIR card, which utilises a flavour of 3DS 1.0.2 compatible with Visa’s standard for cardholder authentication, was released by the Russian Central Bank’s subsidiary, NSPK, to combat sanctions imposed by Europe and the USA, and prevent any other external economic or political factors from influencing the in-country processing of card payments.

In 2015, Visa and Mastercard joined with MIR creating co-branded cards. Since then, agreements have been signed for Russian banks to issue Mir-Maestro, Mir-JCB, Mir-AMEX and MIR-UnionPay cards. Within Russia, these cards will function as MIR cards. When used outside of Russia, they will operate in the same way as standard cards in the international payment systems of their co-brands.

NSPK is expecting to issue 120 million MIR cards by 2019 and its commitment to entering the international market was demonstrated when it joined EMVCo as a business and technological partner, in 2015, to be able to actively participate in EMVCo working groups for the creation, development, promotion and implementation of international standards.18

18 Plus Journal, “Russian Payment Market on the move”:
http://www.plusworld.org/features/russian-payment-market-in-on-the-move/
Asia Pacific

Asia Pacific, along with the rest of the world, is seeing card payment amounts increasing. In the next five years, analysts, McKinsey, are expecting the Asian market to account for 50% of the global payments, with strong growth in the use of smartphones for online payments.

Across Asia, a number of schemes have been incorporated to handle the increase in card-not-present transactions online. In Thailand, the national e-payment system came into operation on 1 January 2017 to encourage the use of identification numbers or mobile numbers to perform transactions. Such schemes are being hailed as next generation payment systems.


PSD2 Directive (Europe)

PSD2 is an update to the original Directive on Payment Services (PSD) issued by the European Commission. The directive offers a framework for safer payments across Europe. The first version of this directive was released on 1 November 2009, and the updated version came into force on 8 October 2015. PSD2 allows for a more risk-based approach to payment authentication, whilst ensuring that strong authentication is used as de facto for online payments. The ultimate goal is to reduce fraud, whilst also offering better levels of usability. The 3D Secure payment authentication standard, used by Mastercard, Visa and others within Europe, complies with the requirements of the PDS2 framework. Service providers, such as Mastercard, are also exploring the use of biometrics to balance security requirements with usability. Mastercard is expecting to improve payment approvals from 80% for remote transactions to that of face-to-face approvals, which stand at around 96%.


CONCLUDING THOUGHTS

Authentication during card-not-present online transactions is important on a number of levels. It builds a trusted relationship between the merchant and the customer, but importantly, it is another way of improving security in a world where cyber security has become a major issue.

3D Secure is a major authentication standard in use across Europe and Asia, with much less traction in the USA. It is expected to become even more widely used once the new ‘frictionless flow’ version 2.0 is implemented. 3D Secure is, however, unlikely to become the worldwide standard for payment authentication as in-country processing standards have entered the market in countries such as India, China, Russia and Thailand, countries in which phenomenal growth in online transactions is expected over the next few years.

The 3D Secure 2.0 standard, in its current form, enforces the capturing of a significant amount of private cardholder data, to support risk-based authentication by the issuer. As this personal information is collected by the respective card schemes and the standard does not stipulate to what extent they can access it or across which country and regional borders they can transfer it, it may raise questions of privacy and data sovereignty at all levels from cardholder to government. Although issuers and merchants are expected to support both 3DS 1.0.2 and 3DS 2.0 during the transition period, the standard fails to provide protection for existing investments made by banks and merchants in support of the original 3DS 1.0.2 standard by not providing interoperability between the two standards. These factors may further influence the fragmentation of payment authentication standards by encouraging the development of more regional or in-country standards.

It is our expectation that in the coming years, 3DS 2.0 will have a key role to play together with other payer authentication standards. As a consequence, card issuers, payment service providers, online merchants, and providers of payment authentication software, will need to adapt and support multiple authentication standards in order to facilitate the global growth of secure online payments.