Global Payment Authentication Standards

GPayments

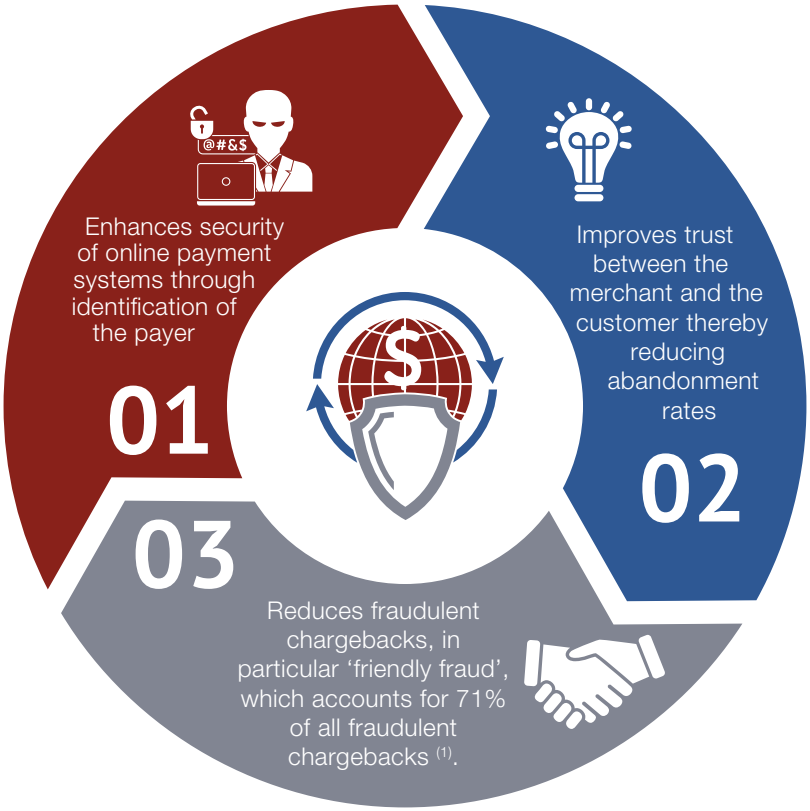
AUTHENTICATION, SECURITY AND PAYMENT SOLUTIONS

CONTENTS

GLOBAL PAYMENT AUTHENTICATION STANDARDS

In today's eCommerce environment, it has become crucial to authenticate payers during card not present transactions. Payment authentication standards enable this by providing an additional layer of protection, in the form of an authentication step. In the course of a transaction, the online payer will be requested to enter unique authentication data, for instance a static or one-time password, associated with the account in use. The result of the authentication indicates whether the payer is the genuine owner of the account.

The adoption of payment authentication standards offers imperative benefits:

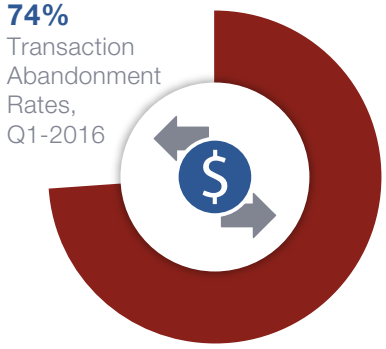


These payment authentication standards have been developed by card brands, financial institutions, and consortia such as EMVCo, the National Payments Corporation of India, The National Payment Card System (NPCS) of Russia, and the European Commission. EMVCo, for instance, is a cross-industry corporation with six member organisations: American Express, Discover, JCB, MasterCard, UnionPay, and Visa, that promotes the global acceptance of such standards within the payment industry. EMV, a technical standard for smart payment cards, was introduced in 1994 by EuroPay, MasterCard, and Visa, with the goal of reducing card fraud. In recent years, EMVCO has facilitated the development the latest version (2.0) of the widely accepted 3D Secure standard. Additionally, in recent years, in-country processing standards have entered the industry from various regions of the world, with China, India, and Russia introducing UnionPay, PaySecure, and MIR, respectively.

1. Ethoca Payment Network, "Stopping Fraud, Accepting More Transactions": *https://macmember.org/library/public/Ethoca.pdf*

WHY THERE IS A NEED FOR THESE STANDARDS

Global eCommerce is expected to be in the region of $2.4 trillion by 2019, with credit cards being the most used method of payment across all regions of the world. [1] This increase in online spending comes with an increase in fraud. Juniper Research, in a recent report, found that online transaction fraud is likely to increase to $25 billion USD by 2020 [2]. This poses a big problem for the industry and one which needs to be addressed by enforcing security at the point of payment. Payment authentication standards were designed for online payments, to prevent fraudulent online transactions by adding a layer of security to the process of payment authorisation. Additionally, this added security allows customers to pay with confidence, resulting in a positive impact on transaction abandonment rates, which were found to be over 74% in Q1 2016 [3].



1. WorldPay, Global Payments Report Preview: *http://offers.worldpayglobal.com/rs/850-JOA-856/images/GlobalPaymentsReportNov2015.pdf*

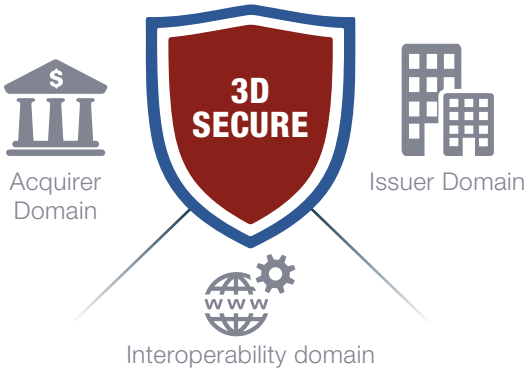
2. Juniper Research, ONLINE TRANSACTION FRAUD TO MORE THAN DOUBLE TO $25BN BY 2020: *https://www.juniperresearch.com/press/press-releases/online-transaction-fraud-to-more-than-double-to-$2*

3. Salescycle, The Remarketing Report: *https://blog.salecycle.com/stats/infographic-the-remarketing-report-q1-2016/*

USAGE OF PAYMENT AUTHENTICATION STANDARDS

3D Secure (Worldwide)

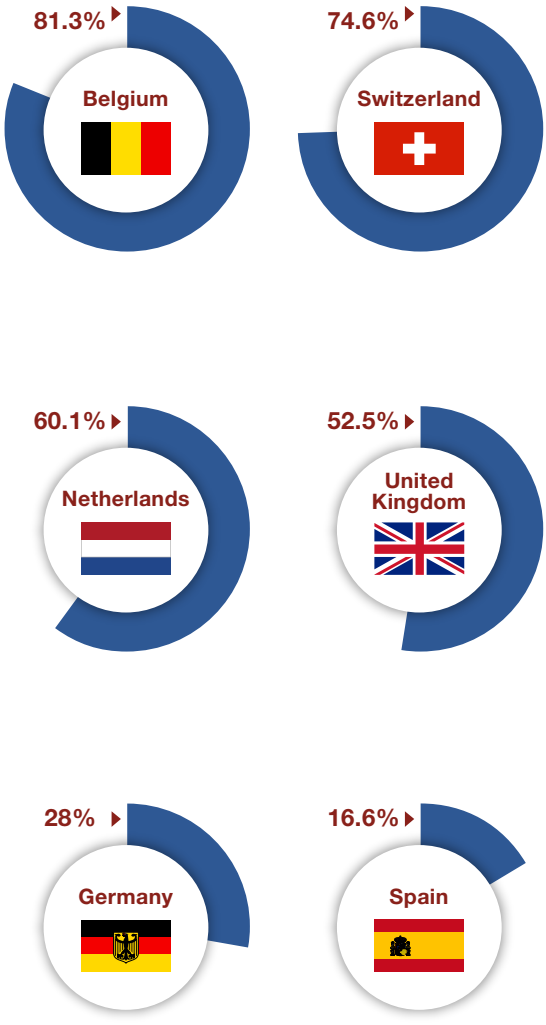
3D Secure, or 3 Domain Secure, is so named because of the three domains involved in payment transactions. The domains are the Issuer domain of the card issuing bank, the Interoperability domain of the card scheme's infrastructure and the Acquirer domain of the merchants and banks to which payment is being made. 3D Secure was originally developed by Visa in 2001 and branded as 'Verified by Visa.' It was extended to include mobile payments in 2005 [1]. MasterCard initially experimented with 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 has to also implement the use of 3D Secure within their site, installing a Merchant Plug-in (MPI). The MPI communicates with the bank 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 itself approved, the payment will be made and the transaction completed.

One of the big selling points of 3D Secure is that it offers the merchant full liability against fraudulent transactions. The thought being that if a user has to pass through another layer of authentication to authorize a transaction, it becomes less likely that the card is being used in a fraudulent manner.

3D Secure is used throughout the world; however, it is not used uniformly and 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 (2):



The number of successfully authenticated transactions within these countries was high; varying from 95% to greater than 98%, showing that the method is robust.

Moreover, from a marketing perspective, transaction conversion rates are affected by implementations of 3D Secure, due to the possibility of transaction abandonment by the cardholder. The level of impact has varied greatly among different countries. A report by Ayden, exploring conversion rates for merchants implementing 3D Secure, found that in the United Kingdom conversion rates only suffered by around 2.5%, whereas in China and the USA, 3D Secure negatively impacted conversion rates by 43% (3). 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.

1. Business Wire,"Arcot Systems to Offer 3-D Secure(TM) with Visa International... ", Dec 13 2005: *http://www.businesswire.com/news/home/20051213005963/en/Arcot-Systems-Offer-3-D-Secure-TM-Visa*

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

3. Ayden, "Adyen Analysis Reveals Worldwide Impact of 3D Secure on Transaction Conversion Rates": *https://www.adyen.com/press-and-media/press-releases/press-release-detail/2014/adyen-analysis-reveals-worldwide-impact-of-3d-secure-on-transaction-conversion-rates*

3D Secure 2.0 (Worldwide)

The redesigned specification for 3D Secure, version 2.0, was released by EMVCo in October 2016 [1]. Since the first version of 3D Secure was released in 2001, there have been many changes to the way online payments are made. The specification of 3D Secure 2.0 has been built to provide support for:

Native mobile based payments

Integration with browsers and mobile apps

Risk-based authentication to optimize security

Multiple-factor authentication options

Digital wallets

3D Secure 2.0 aims to offer a more frictionless, seamless, and user friendly experience. Cross-platform support allows merchants to offer an extended sales platform and ensures a more secure purchasing process. A major limitation of the new specification, however, is the standard's lack of interoperability and support for coexistence of 3D Secure 2.0 with 3D Secure 1.0.2 and other in-country standards such as India's PaySecure, China's UnionPay, and Russia's MIR. The new specification is also relatively US-centric and does not address the need to have open interoperable global standards, which will lead to further fragmentation of the payment authentication arena. The introduction of 3D Secure 2.0 is a missed opportunity for creating a global standard to embrace the needs the payment authentication marketplace.

3D Secure 2.0 implementation is being supported through the EMVCo community and additionally, the PCI Security Standards Council will be using the new specification as part of its information security requirements framework. Visa has announced it proposes to set a deadline for card issuers and merchants to migrate to version 2.0 between April and October 2018 across various world locations [2].

1. EMVCo, EMV 3D Secure 2.0: *http://emvco.com/specifications.aspx?id=299*

2. isa, Online Authentication 2.0: Improving Security in e-Commerce: *https://usa.visa.com/visa-everywhere/security/improving-security-in-ecommerce.html*

PaySecure (India)

India's online transactions accounted for 14% of its total transactions in 2014, which is anticipated to increase as more people take up the use of smartphones [1]. eCommerce in India is expected to be worth $100 billion USD by 2020 [2].

As a result, the National Payments Corporation of India, a not-for-profits organization, has developed a domestic card framework payment system for India, which has been branded as RuPay card. In a similar manner to the 3-D Secure standard, the RuPay card 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. Transactions over a certain limit will require a one-time password (OTP), sent to the user's registered mobile number, email address or device, before entering their card's PIN.

Furthermore, an anti-phishing mechanism is also available for implementation, allowing the user to check their last 3 online purchases during the transaction.

---

1. Daze Info, Online Payment In India Accounted For 14% Of Total Transaction Amount:
https://dazeinfo.com/2015/05/29/online-payment-india-accounted-14-total-transaction-amount-fy-2015-report/

2. 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

UnionPay Online Payments (UPOP) (China)

Online transactions in China have increased year on year to 2.43 trillion Yuan ($353 billion USD) by 2015 [1]. They are expected to reach $1.6 trillion USD by 2020 [2]. UnionPay or UPOP is the standard used by over 50 Chinese financial institutions, to provide a payment authentication framework for 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 has joined forces with EMVCo and will utilize the 3D Secure 2.0 protocol. SecurePay is another security system that can be used with UnionPay and is provided by over 70 issuing banks in China. When a payer is registered for SecurePay, they are redirected to the issuing bank's site to authenticate themselves using an OTP sent to their mobile number.

1. Statistica, Total online payment transactions in China in 2014:
https://www.statista.com/statistics/490192/total-online-payment-transactions-in-china/

2. Bain and Company, E-commerce in China reaches a record high penetration:
http://www.bain.com/about/press/press-releases/China-ecommerce-2015-press-release.aspx

MIR (Russia)

The MIR national payment card was released in Russia as a result of sanctions imposed on Russia by Europe and the USA. Visa and MasterCard joined the MIR card, creating co-branded cards, enabling in-country processing of payments in 2015. UnionPay has also signed an agreement to create a joint UnionPay-MIR card.

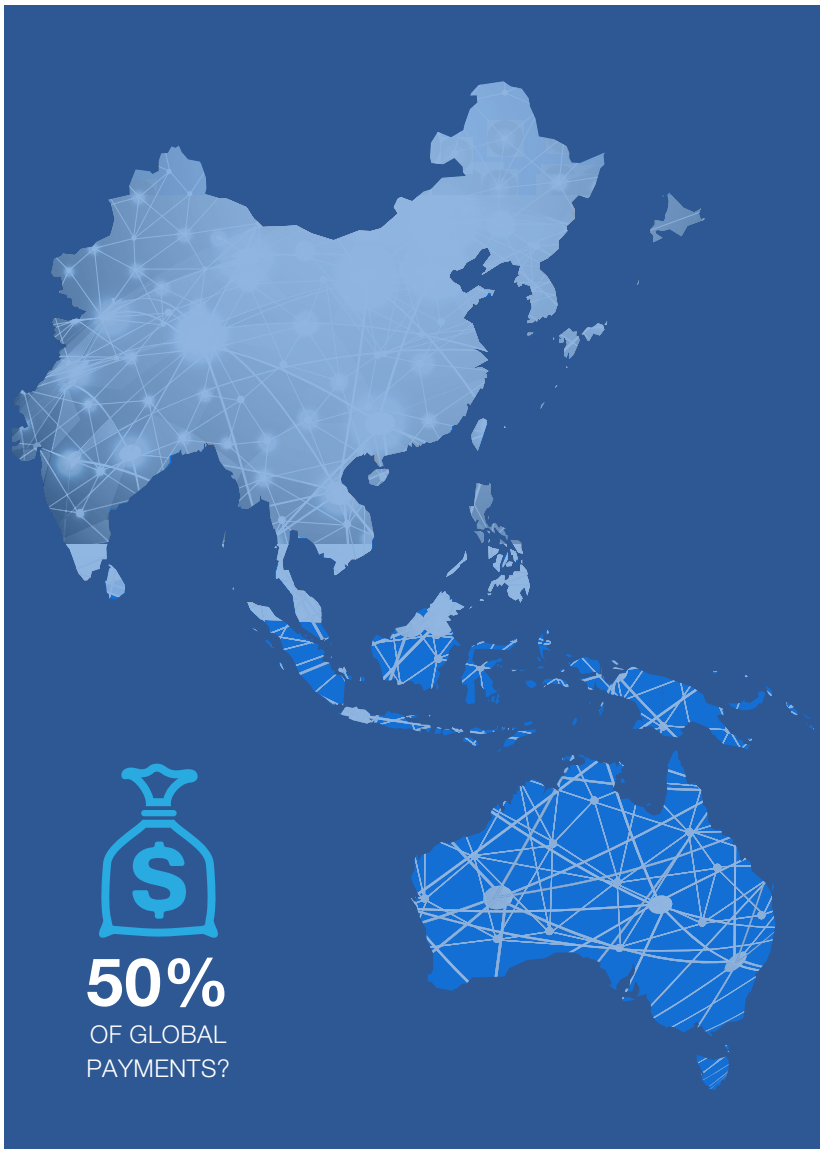
The National Payment Card System (NPCS) is expecting to issue 120 million MIR cards by 2019. [1]

1. 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 [1]. In the next 5 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 [2].

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 is expected to come into operation on January 1st, 2017 to encourage the use of identification numbers or mobile numbers to perform transactions. Such schemes are being hailed as next generation payment systems.



1. Bloomberg, Digital Payments are Shaking up Asia's Credit Card Industry: *http://www.bloomberg.com/news/articles/2016-08-18/idle-credit-cards-in-asians-wallets-prompt-citi-hsbc-overhaul#media-2*

2. McKinsey, Insights from McKinsey's Asia-Pacific Payments Map, Sept. 2012

PSD2 Directive (Europe)

PSD2 is an update to the original Directive on Payment Services (PSD) issued by the European Commission. [1] The directive offers a framework for safer payments across Europe. The first version of this directive was released on 1st 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 against 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%. [2]

1. (1) European Commission, Directive on Payment Services: *http://ec.europa.eu/finance/payments/framework/index_en.htm*

2. MasterCard, E-commerce Transactions – A New Roadmap for authentication in Europe: http://newsroom.mastercard.com/wp-content/uploads/2015/07/A-New-Roadmap-for-Authentication-in-Europe.pdf

Concluding thoughts

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

3D Secure is a major authentication standard in use across Europe and Asia, in countries such as Belgium, Switzerland, Japan, Singapore and Vietnam, with much smaller 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 de facto standard for payment authentication, as in-country processing standards have entered the market in countries such as India (PaySecure), China (UnionPay), Russia (MIR), and Thailand (national e-payment system); 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, has failed to provide protection for existing investments made by banks and merchants in support of the original 3D Secure 1.0.2 standard. This, along with the lack of interoperability with its previous version, may further influence the fragmentation of payment authentication standards by encouraging the development of more in-country standards. It is expected that in the coming years, 3-D Secure 2.0 will have a key role to play among other standards.

As a consequence of the market utilizing multiple payer authentication standards, card issuers, 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.

For more details, Download

PRODUCT 1

DOWNLOAD

PRODUCT 2

DOWNLOAD

GPayments

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book.