tas group
an owl company

White Paper

3-D Secure 2

Optimize the buying experience, increase sales, reduce fraud

www.tasgroup.eu

Index

Contents

1. Introduction

Customer authentication has never been more important with online payments continuing to grow a pace year on year, and with them rising CNP fraud losses. According to The Nilson Report, CNP fraud accounts for over half (54%) of all fraud losses, yet CNP purchases make up less than 15% of all card sales. With fraud losses worldwide reaching $28.65 billion in 2019 and projected to rise to a staggering $35.67 billion in five years, it's clear that the payments industry has some formidable challenges ahead.

Today cardholders expect seamless, fast payments and are looking for ultimate convenience and ease in their buying experience. Issuers, merchants and PSPs are therefore tasked with striking the right balance between delivering a positive buying experience, while at the same time mitigating this increased fraud risk. Having a strong authentication strategy is key to effectively striking this balance.

3-D Secure is one such way to achieve this. However, considering the continuous rise in digital commerce and pressure from consumers today for a secure, frictionless payment experience, it's clear that the original protocol, 3-D Secure 1 (3DS1), developed some 20 years ago, is no longer fit for purpose. So, out of a pressing need to make buying safer, reduce shopping cart abandonment while improving the overall customer experience, EMV 3-D Secure 2 (3DS2) was born.

2. The new 3-D Secure

Better informed to make better decisions

3-D Secure 2 (3DS2), is the new protocol introduced in 2016 by EMVCo – the global technical body governed by the card networks – and is designed not only to make purchasing online much more secure and reliable but to enhance the overall customer buying experience.

3DS2 does this by bringing real intelligence to cardholder authentication, facilitating a far richer exchange of data between the issuer, the acquirer and the payment scheme. By making use of over 100 potential data points (10 times more than was supported by 3DS1), such as amount, device, IP address, email address, location, MCC, delivery details, account age, this new protocol enables frictionless flows wherever possible. As cardholders are subject to fewer authentication challenges, the checkout process is quicker, resulting in lower cart abandonment and more sales conversions. 3DS2 also allows soft-declines, something its predecessor didn't, which avoids the merchant having to start the transaction from scratch should the issuer deem authentication necessary, again reducing the likelihood of the customer abandoning the purchase.

By evaluating this additional transactional, behavioural and contextual data, issuers can carry out Risk-based Authentication (RBA) powered by advanced analytics to make smarter authentication decisions. Machine learning can also be exploited to better assess the risk profile of the transaction and decide whether to prompt further cardholder challenges, or not.

With around 95% of online transactions deemed to be low risk, and just 5% thought to be higher risk according to Visa, it makes perfect sense to carry out this analysis behind the scenes and only invoke authentication challenges on this latter category. This is the power of RBA. A risk-based approach to fraud monitoring has indeed already proven effective. A Visa Europe study performed over the last few years in the UK found that where PSPs have been using RBA, benefits are enjoyed by all parties.

3DS2 delivers a secure, seamless and consistent user experience across all digital payment channels: the 3DS2 protocol is designed to support today's digital payments, providing reliable, intelligent authentication across all devices including smart phones, tablets, wearables, supporting in-app purchases, tokenization and digital wallets and enables the use of dynamic authentication through biometrics and token-based authentication methods.

3. 3-D Secure 2: the benefits

Benefits for Acquirers and PSPs:

- **Increased security, lower fraud rates** – more possibility to apply SCA exemption (in Europe)

- **Lower cart abandonment, higher conversion rates** – delivers an improved customer experience with reduced friction and more sales conversions, increasing acquirer / PSP revenue

- **Reduced costs** – protects the acquirer/PSP from fraud-related chargebacks, reducing chargeback handling costs

- **Allows easy compliance with network ecommerce authentication mandates**

Benefits for Merchants:

- **Increased conversion and sales** – by enhancing the customer experience, allowing a faster, frictionless checkout experience, merchants can expect fewer drop offs and more conversions. 3DS v 2.2 allows merchants to request exemptions through their acquirer

- 3DS2 has been shown to speed up the purchasing process with an **85% reduction in checkout time and a 70% reduction in cart abandonments** from 4% to under 1%. Source: Visa

- Unlike 3DS1, **3DS2 can be used to set up merchant-initiated** transactions (useful for enabling recurring payments such as subscriptions)

- **Higher authorization rates** – approval rates shown to be 10 to 11% higher in markets where 3DS2 is used

- **Fewer chargebacks lower operational expenses** – Increased security reduces the risk of fraudulent transactions and decreases the number of disputed transactions. Additionally, thanks to a richer data exchange, merchants are armed with more information to challenge any disputes

- **Lower transaction fees** - by adopting 3DS2, merchants and acquirers enjoy a reduction in transaction fees

- **Fewer false positives** - 3DS2 reduces the number of false positives saving lost revenue each year, not to mention avoiding the costly fallout from the negative customer experience

Benefits for Issuers:

- **Better customer experience / fewer false positives** – 3DS2 lets issuers perform seamless, background user authentication thanks to a richer data exchange that can be run through the bank's risk analysis and fraud prevention engines, thereby reducing false positives and unhappy customers

- **Fewer chargebacks and lower operational expenses** – Increased security reduces the risk of fraudulent transactions and decreases the number of disputed transactions

- **Richer data for targeted cross-selling and customisation** – Issuers can leverage the rich amount of new data related to their customers' purchasing behaviours to develop customized services, and upsell targeted propositions to cardholders

- **Allows easy compliance with network ecommerce authentication mandates**

4. 3DS2: a smart way to support SCA and its exemptions

In Europe, the Revised Payment Services Directive (PSD2), which requires banks to open their customer data assets to third parties, mandates the adoption of Strong Customer Authentication (SCA) to enhance payment security. SCA, which **came into force in Europe on 31 December 2020**, requires that two of three different authentication factors are provided – so something the customer has in their possession, something they know and something they are.

By enabling 3DS2, businesses can easily comply with this SCA requirement for online payments.

SCA EXEMPTION

A major downside to SCA is that it reintroduces the friction that all parties were trying to eliminate. Luckily there are some instances where PSPS and banks can skip SCA and avoid unnecessary customer friction by applying something called a SCA exemption. For online payments under PSD2, SCA exemptions are allowed on transactions that are:

- Low value and/or
- Low risk

Transactions up to a certain € value, dependent on the payment provider's overall fraud levels (see table), up to €500, are exempt from SCA. No SCA is required for transactions below €30.

SOMETHING THE CUSTOMER

KNOWS	OWNS	IS
Pin Password Secret fact	Token Mobile phone Wearable device	Iris format Fingerprint Facial features

Exemption Threshold Value	Fraud rate exemptions (%) Remote card-based payments
500 EUROS	0.01
250 EUROS	0.06
100 EUROS	0.13
30 EUROS	EXEMPT

Note: certain types of transactions, such as recurring plans and subscriptions, do not require SCA to be performed once the first transaction has been authenticated.

However SCA will be required if five or more exempt transactions have been performed on the same card or payment method in a 24-hour period or if these exempted transactions total more than €100.

One way that merchants can ensure a good buying experience through the new 3DS2 protocol is by encouraging their customers to place them on a whitelist of “Trusted Beneficiaries”, which is maintained by the issuing bank. Once whitelisted, merchants will be exempt from 3-D Secure following the first purchase. It’s worth noting that placing merchants on a whitelist can only be done by the issuer.

It is important to note that under PSD2, merchants may not apply SCA exemption by themselves. Only issuers and acquirers can do so. However, merchants can agree bilaterally with their acquirer to share liability risk and provide the information to enable them to apply the exemption.

5. 2.1 v 2.2: how do they compare?

3DS 2.1 and 2.2: an evolution towards the optimal buying experience

While the changes from the original 3DS1 to 3DS2 were considerable, delivering a far superior user experience by introducing frictionless authentication, shorter transaction times and consequently greatly improved sales conversions, the newest version 2.2 builds upon the previous version, 2.1, and includes a number of important new enhancements to promote an optimised consumer experience during ecommerce transactions.

With version 2.2 **merchants and PSPs are able to request SCA exemptions through their acquirer** by applying **Transaction Risk Analysis (TRA)** to demonstrate that the transaction is low risk. Version 2.2 also supports **merchant whitelisting**, where a merchant is added to a Trusted Beneficiary list by the cardholder allowing them to process transactions from this cardholder without SCA. Another new feature is **delegated authentication**, where an issuer permits a merchant, acquirer or PSP to perform the authentication, and lastly, version 2.2 also supports **decoupled authentications**, where a user performs authentication using a method outside of the main 3DS authentication flow, authenticating themselves, for example, on their mobile device, to allow for authorization on another device, such as their computer.

Are you vulnerable to liability shift changes?

From October 2021 3DS1 will start to be decommissioned by the card schemes meaning that merchants relying on this version will no longer be sheltered from liability for fraudulent transactions. It is therefore recommended that a move to 3DS2 is on their 2021 roadmap, and that they start the upgrade process as soon as possible.

What is new in EMV 3DS 2.2.0

EMV 3DS 2.2.0 delivers the following key features that are not available in previous versions of 3-D Secure.

Versions compared:

Notable Features	3DS 1.0	EMV 3DS 2.1.0	EMV 3DS 2.2.0
Out-of-Band (OOB)/Biometric Mobile banking app integration	N	Basic	Y
3DS Requestor Environment - 3RI			
• Non Payment authentication	N	Y	Y
• Payment authentication with ability to obtain, refresh and regenerate CAVV	N	Y	Y
• Decoupled authentication	N	N	Y
Acquirer Exemption indicators			
• Transaction Risk Analysis (TRA) performed prior to authentication	N	N	Y
• Trusted beneficiaries (whitelisting)	N	N	Y
• Delegated Authentication	N	N	Y
Additional device compatibility e.g. gaming consoles	N	Y	Y

Source: Visa.co.uk

6. TAS 3-D Secure 2: using compliance to build a better customer experience

TAS offers fully customizable 3-D Secure solutions for both Issuers and Acquirers (Merchants, Gateways, PSPs and Processors) that allow you to create custom authentication experiences and shrink online fraud.

TAS 3DS Access Control Server (ACS) and Directory Server (DS) 2

Access Control Server (ACS) and Directory Server (DS) 2 are the latest versions of the 3-D Secure (3DS2) software packages developed by TAS. They enable issuers, acquirers and PSPs to optimize the end user experience during ecommerce shopping and to authenticate cardholders, by eliminating friction and increasing conversion rates, while helping to reduce fraud. Both solutions fully support the latest EMVCo 2 standards.

Completely based on Open Standards and designed to address the current and emerging worldwide payment market.

TAS 3DS2 solutions:

- **easily integrate with existing payment infrastructures via APIs**
- **provide unparalleled flexibility and choice on the market, offering on-premise license, SaaS or hybrid cloud delivery options.**

ON THE ISSUING SIDE

For Issuers, PSPs, Processors, Program Managers

TAS 3DS solution for issuers includes the Access Control Server (ACS) that implements the new EMVCo 3-D Secure 2 specifications + Risk Based Authentication (RBA) and supports:

- Enrolment of cardholders
- Directory Server (DS) authentication request processing
- Strong customer authentication (SCA) – frictionless and challenge flows
- RBA for SCA exemption
- Non-payment authentication
- Out-of-band (OOB) authentication
- SMS OTP
- Supports fallback to different authentication flow
- Whitelisting
- Decoupled authentication
- New 3DS Requestor Initiated (3RI) indicator

ON THE ACQUIRING SIDE
For Acquirers, PSPs, Processors, Gateways, ISOs, Merchants

TAS 3DS solution for merchants and acquirers includes the 3DS Server + 3DS SDK and supports:

- Simple integration with web shops, mobile applications and wallets via Open APIs
- SDK for Android and iOS for Requestor Mobile App implementation
- Frictionless and challenge transaction flows
- Supports all types of ecommerce transactions including recurrent payments, instalments, etc
- Management of multiple acquiring institutions in one 3DS

TAS 3DS2 for smarter customer authentication

Solutions that combine the power of advanced technology with the latest EMVCo standards and 35+ years of payments expertise to build a better, safer buying experience for your customers:

- Integrated RBA module with configurable rules engine to comply with PSD2 TRA requirements to support SCA exemption
- Integrated optional AI/ML based module (Payment Intelligence) analysing cardholder behaviour both for fraud prevention and for marketing insights
- Full microservices processing for building advanced customer experience
- Flexible licensing model
- Compliance with latest EMVCo 3DS specifications and ensuring backward compatibility
- Ease of integration, setup and maintenance – flexible packages

About TAS Group

TAS Group is a leading provider of payments software, delivering innovative solutions for cards and digital payments for over 35 years. With a global reach and offices in 9 countries spanning Europe, North and Latin America, we empower customers around the world to unlock the infinite potential of digital and mobile payments in the open and instant era and play an active role in the new ecosystem.

Our digital payments platform, PayStorm, delivers a modular cloud-native solution to manage card and mobile digital payments in both the Issuing and Acquiring domains. Through a rich set of open APIs, banks and PSPs can easily design and configure next-generation digital payments products and tailor exciting customized user experiences with impressive speed. Our solutions are in production in 20 countries, supporting 8 languages, processing millions of real-time transactions each day.

To learn more about our solutions and services, visit us:

www.tasgroup.eu

solutions@tasgroup.eu

@TAS_Group

TAS Group