3-D Secure 2.0 (3DS 2.0): Putting Customer Experience at the Center of Payment Authentication

Back in the early-to-mid 2000s, Visa introduced the current 3-D Secure protocol (3DS 1.0.2) through its Verified by Visa program, with adoption by the other credit card schemes following. Since this was years before the smart phone was first launched, it’s no surprise that the protocol isn’t designed to provide a good user experience on mobile devices, or to use the latest in authentication methods.

In fact, just five years ago, not much more than 15% of ecommerce traffic was mobile, according to RSA data, whereas today it’s more than 45%. Fraud in the mobile channel has grown along with — indeed, faster than — the growth in mcommerce (see Figure 1). Responding to this sea-change, as well as to the proliferation of digital wallets and in-app purchases, EMVCo\(^2\) has developed 3-D Secure 2.0 (3DS 2.0).

The revised protocol has been designed from the start to address the chief criticisms attracted by 3DS 1.0.2, particularly with respect to eliminating sources of friction for shoppers. It aims to deliver a much smoother authentication experience — in fact, largely a completely frictionless one — while also doing better to secure transactions against fraud.

This paper explains the key things you need to know about 3D Secure 2.0 including:

- Defining features and why they matter
- The benefits of adoption for issuers and merchants
- What issuers should consider when choosing a 3DS 2.0 authentication provider

---

1 Including MasterCard SecureCode, JCB J/Secure, and American Express SafeKey.
2 EMVCo is jointly owned by American Express, Discover, JCB, MasterCard, UnionPay, and Visa. It is responsible for the development of 3-D Secure as well as the EMV standard.
3DS 2.0 features and why they matter

A recent study conducted by Visa Research found that 72% of online shoppers have abandoned a virtual shopping cart over fear of security concerns. This has been the inevitable hurdle with 3D Secure and its lack of mass adoption – how to balance security and convenience to avoid shopping cart abandonment. Consumer convenience most often won out with merchants more willing to take the risk of a chargeback than an abandoned shopping cart.

3DS 2.0 is putting the shopper’s experience of authentication front and center. The protocol may be fundamentally about security and fraud prevention, but it approaches its objective from the perspective of genuine customers.

After all, card schemes, issuers and merchants all need happy customers. And however serious fraud gets, genuine transactions will always vastly outnumber fraudulent ones. So 3DS 2.0 is designed to improve payment security for customers, without negatively affecting their shopping experience. It does this through five key features.

• Elimination of active enrollment

Shoppers will no longer see confusing and hugely inconvenient popups asking them to register their card with a security scheme. Instead, participating issuers will enroll all of their cards when they sign up to a 3DS 2.0 scheme.

This automatic card enrollment is possible because card users no longer need to set an authentication password (see feature 4). The removal of active enrollment eliminates a major source of customer friction in the existing 3DS specification.

• Data-rich authentication

Merchants will deliver much more data with each transaction than is currently required for 3DS 1.0.2. Examples include
Merchant Category Code (MCC), merchant risk indicator, and key addresses (shipping, billing, email), among many more.

This increase in data richness is at the very heart of a largely frictionless 3DS 2.0 experience for shoppers. Issuers will use this richer data to facilitate more accurate fraud risk assessment via their Access Control Server (ACS) providers. And more accurate fraud risk assessments will enable acceptance of more orders without challenge.

- **Cross-channel, device-agnostic support**

  Merchants can ensure that on the rare occasion a challenge is required, the experience is much more seamless for their customers. Unlike the traditional popups and redirects that cause friction and uncertainty (and work poorly on mobile devices), the new specification allows for complete integration with the shopping experience, irrespective of the device being used. Merchants can use software development kits (SDKs) to integrate authentication screens with their desktop and mobile sites, mobile apps, or indeed smart TVs, watches, other wearables and gaming consoles — 3DS 2.0 is ready for the 'Internet of Things', supporting IoT devices and the payment methods they use.

- **Smarter, broader authentication**

  Static passwords, too easily compromised, are no longer allowed. Instead, 3DS 2.0 requires dynamic authentication methods such as one-time passwords and biometric ID, and also supports out-of-band authentication (for example, authenticating a desktop session with a one-time code sent to a mobile device). This means that if a shopper is challenged, the process is as convenient as possible for them.

  Responding to developments in payment methods, 3DS 2.0 also extends authentication to in-app purchases and digital wallets that store card details, and it can also be used in a non-payment scenario, such as when a customer adds a new card to a digital wallet.

- **Faster all around**

  3DS 2.0 offers performance improvements for end-to-end processing. Add this to better integration with merchant sites and apps, and smarter authentication methods, and the whole process becomes smoother and faster.

  Through these changes, 3DS 2.0 comprehensively addresses the concerns merchants have with 3DS 1.0.2. With clear benefits to adoption (see below) and their concerns addressed, we expect uptake of 3DS 2.0 among merchants to be considerably more enthusiastic than it has been for 3DS 1.0.2. As merchants adopt 3DS 2.0, issuers need to be ready to support the protocol — or accept the liability shift without benefit of data-rich fraud detection. And there are other good reasons to adopt 3DS 2.0.
Benefits of 3DS 2.0 adoption
For merchants, the main benefits of 3DS 2.0 are essentially the same as offered by 3DS 1.0.2 — and this time without any negatives to potentially outweigh the positives. Some of these include:

- Liability shift for every transaction passed through the 3DS process
- Lower interchange fees
- Higher authorization rates from issuers
- Ability to customize the look and feel of the 3DS experience
- Smoother shopping experience for customers, including no enrollment, no passwords and support for mobile applications and smart devices.

Overall, there are several other benefits that accrue to both merchants and issuers.

Positive customer experience and revenue growth
Adoption of online and mobile services has consistently shown a positive growth pattern with the addition of security controls such as risk-based authentication.

One large bank, focused on transforming security for its online and mobile banking applications, found that the introduction of security quickly led to:

- 20% increase in its customer base
- 40% growth in use of online services
- 60% growth in mobile banking users

This is one example illustrating a general principle that when online businesses give their customers an experience that is both faster (no delay in pages loading, for example) and more secure, they attract and retain more customers, and customers transact more online.

Better fraud prevention
Issuers are the clearest beneficiaries of the greater exchange of data required by 3DS 2.0. The more data they have, the more accurately they can assess transaction risk, and since issuers are the ones taking on liability for any chargebacks, more complete risk assessment is welcome.

Merchants benefit too, though — especially if they’re not already collecting the kind of rich data that 3DS participation will require, because then they can use this data to improve their own fraud detection efforts. But even if a merchant already has a sophisticated fraud prevention program, the extra layer of protection afforded by the issuer doing their own risk assessment should not be overlooked.

The ACS providers used by issuers generally have access to sources of fraud data that individual merchants may not, often enabling them to deliver a more reliable assessment of fraud risk.

3 RSA, Landsbankinn detects more fraud, grows online banking with the RSA Fraud and Risk Intelligence portfolio, July 2016
Regulatory considerations

There is no shortage of national and industry-related regulations that call for robust information security measures for payments and financial transactions that are designed to protect customers against identity theft and fraud. The 3DS 2.0 specification addresses many of the same requirements called for in most regulations.

The EU’s Revised Directive on Payment Services (PSD2) requirement for strong customer authentication (SCA) is one instance. The adoption of 3DS 2.0 could potentially help payment providers minimize the impact of the SCA requirements. For example, the authentication methods supported by 3DS 2.0 are similar to the requirements for SCA as defined by PSD2.

Considerations for selecting a 3DS 2.0 authentication provider

To take advantage of the opportunities afforded by 3DS 2.0, issuers need a customer authentication provider that can be relied on to make the most of the specification. The following factors provide a good checklist to get started.

Fraud detection

With its delivery of richer data, 3DS 2.0 holds out the prospect of more accurate identification of fraudulent transactions. But what does ‘better’ look like? Issuers may want to understand what the provider can achieve today, as a basis for comparison, so it’s worth asking:

- What is the fraud detection rate across various rates of intervention (e.g., step-up authentication)?
- What is the average fraud rate experienced by their customers?
- What about rates for your type of business, in the regions where you operate?

Genuine orders challenged

The flip side of the fraud detection coin is false positives: the number of genuine orders rejected (along with their revenue, and potentially lifetime revenue) after being mistakenly identified as fraud.

ACS providers typically don’t reject orders themselves, since that’s ultimately down to the issuer. Issuers should therefore investigate the number of transactions that a provider intervenes on, that are then accepted by the issuer after further authentication or review, or are rejected but turn out to be genuine (the latter being notoriously hard to measure).

Mobile first

It’s no coincidence that so much of the development of 3DS 2.0 has been driven by mobile: the fastest-growing online shopping and payment channel, and the fastest growing target for fraud. So it’s essential for an authentication provider to have a mobile-first strategy themselves. Considerations may include factors
such as whether the provider offers a user-friendly mobile SDK and risk models to address a variety of channels.

Choice of authentication methods

Consumers aren’t shy about switching loyalties when their convenience is on the line, so it’s vital to support multiple channels and emerging authentication methods. Questions to ask could include:

- What biometric authentication methods are supported and how reliable are they?
- What other authentication methods are supported?

RSA 3D Secure 2.0 solutions for issuers

As an ACS provider for the 3DS 1.0.2 protocol, RSA Adaptive Authentication for eCommerce has already been delivering on many of the benefits of the new specification for nearly a decade. For example, RSA’s risk-based approach eliminates cardholder enrollment, static passwords, and the 100% challenge rate to provide a largely frictionless experience. It supports both fingerprint and eyeprint authentication technologies, transaction signing, and out-of-band authentication with SMS and push OTP, among other authentication methods.

It works across web and mobile channels, bringing together information about behaviors, devices, and known fraud to minimize losses from high-risk transactions.

The RSA Risk Engine at the heart of the service analyzes more than 100 fraud indicators to assess transaction risk. Its risk scores are also informed by the RSA eFraudNetwork, a repository of fraud patterns gleaned from RSA’s research lab, ISPs, third party contributors across the globe, and RSA’s extensive network of customers.

Results

Different customers of RSA Adaptive Authentication for eCommerce have different appetites for risk, and use its policy management functions to translate their risk policies into rules that specify whether any given transaction will be accepted without intervention or not, based on its risk score and other characteristics.

Because of the accuracy of the RSA Risk Engine, users of the service are seeing excellent results. In the first half of 2017, RSA Adaptive Authentication for eCommerce achieved the following:

- **Fraud detection:** A 97% detection rate at a 5% intervention rate (the average intervention rate across the existing customer base). Figure 2 shows detection rates across various levels of intervention (as determined by each organization’s risk policy).

- **Average fraud rate:** 0.035% (3.5 basis points), or just $3.55 loss for every $10,000 in genuine orders approved.

- **Average intervention ratio (Genuine:Fraud):** just 2.4 genuine transactions singled out for every fraud attempt blocked, compared with industry ratios that often fall with the range of 10-20 interventions for every fraud blocked.
Timelines

The following chart represents timelines for the final publication of 3D Secure 2.0 guidelines.

### 3D Secure 2.0 Timelines

<table>
<thead>
<tr>
<th>Date</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 2016</td>
<td>Publication of core 3DS 2.0 specification</td>
</tr>
<tr>
<td>January 2017-present</td>
<td>Additions and clarifications, eg: SDK specification and guide, educational materials, specification updates</td>
</tr>
<tr>
<td>2017-2018</td>
<td>MasterCard has indicated that ACS providers (used by issuers to implement the protocol) will be required to support 3DS 2.0 by the end of 2017. VISA has indicated that European issuers need to be ready for 3DS 2.0 by April 2018. We suspect they will announce a similar requirement, with a later date, for non-European issuers in the near future. Both brands are likely to publish their versions of the 3DS 2.0 guidelines sometime in Q4, 2017.</td>
</tr>
<tr>
<td>Legacy 3DS Support</td>
<td>Support for 3DS 1.0.2 will be withdrawn after a period of parallel running with 3DS 2.0. The specific timing on this is yet to be announced by the various card networks.</td>
</tr>
</tbody>
</table>

Conclusion

Balancing security and convenience in a mobile world is achievable. Risk-based authentication has been helping organizations meet this goal for over a decade. The development of 3DS 2.0 presents issuers with an opportunity to take the lead in delivering a better experience and greater security to their customers. As an EMVCo Technical Associate, RSA was privileged to contribute to the development of the specification, and we look forward to supporting the protocol once the card networks finalize their 3D Secure 2.0 commercial programs.
About RSA

RSA offers business-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change. For more information, go to rsa.com.