From Status Quo To 2.0

The current 3-D Secure protocol

Since the current 3-D Secure protocol (version 1.02) was developed years before the smartphone was first launched, it's no surprise that the protocol isn't designed to provide a good user experience on mobile or internet of things (IoT) devices, nor is it designed to use the latest in authentication methods.

Just three years ago, about 39% of eCommerce was happening on a mobile channel, per RSA data. In early 2017, mobile traffic had grown to over 50% of the total. It grew almost another 10% by mid-2018 (see Figure 1). Interestingly, the portion of online fraud that is happening via mobile channels has grown even faster than mobile transactions, from about 35% in early 2017 to 47% in mid-2018 (a 12% increase) (see Figure 2).

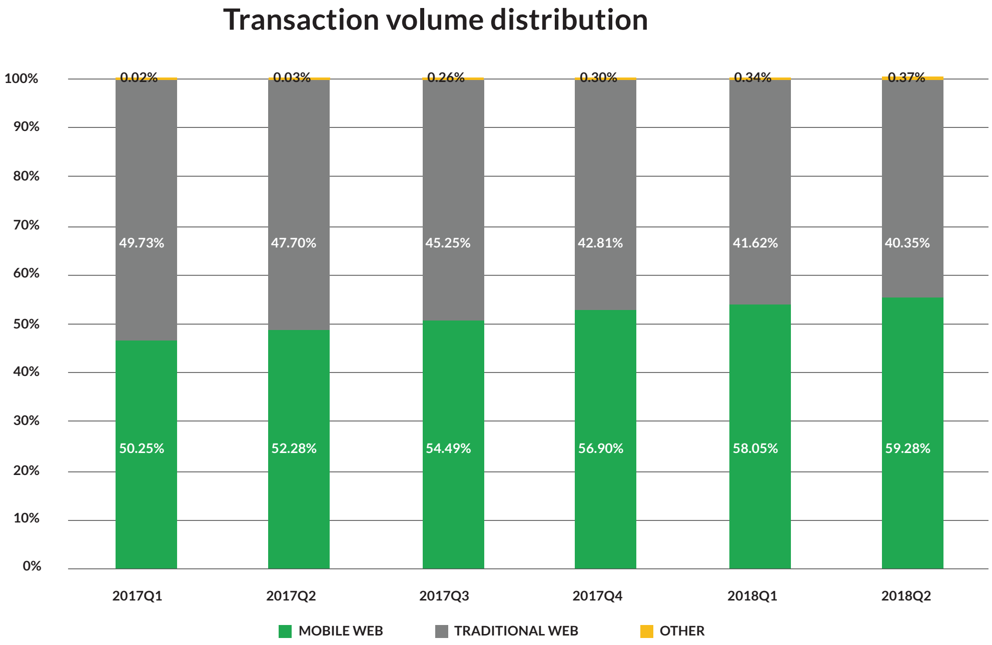


Figure 1: Transaction Volume Distribution. Web vs. Mobile, January 2017—June 2018

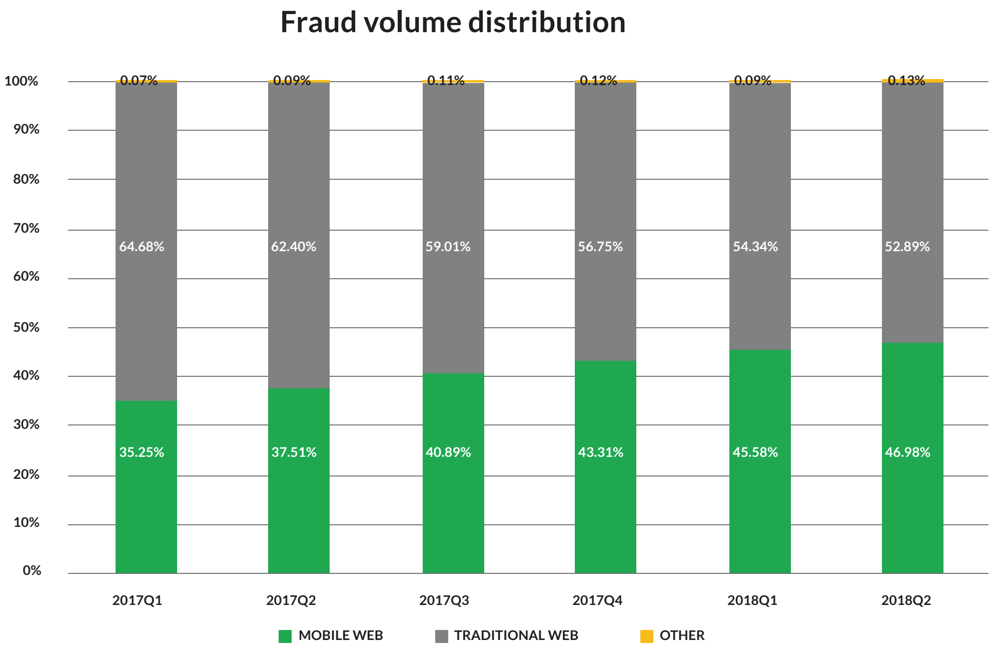


Figure 2: Rates of Traditional Web Fraud vs. Mobile Fraud, January 2017—June 2018

A new solution

Responding to this sea change, as well as to the proliferation of digital wallets and in-app purchases, EMVCo developed EMV 3-D Secure (sometimes referred to as "3-D Secure 2.0", or simply "3DS 2.0").

The revised protocol was designed from the start to address the chief criticisms attracted by 3-D Secure 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:

- The advantages of the current RSA solution vs. standard 3-D Secure
- What's coming with the new protocol
- What you can do to prepare to implement the next generation of 3-D Secure

The RSA advantage

Long before EMVCo created the new 3-D Secure protocol, RSA made enhancements to its Access Control Server (ACS) solution to lessen the negative impacts of standard 3-D Secure implementations. For example, although the standard protocol requires all online shoppers to enroll (either before or during shopping), the RSA offering pre-enrolls shoppers, eliminating much of the friction experienced in the flow. Additionally, rather than require every customer to provide authentication, the RSA risk engine challenges only the riskiest transactions (the global average is about 5%), and yet still stops over 95% of attempted fraud. If you're using our solution today, you're already well aware of these advantages.

What the new protocol brings

The new protocol brings a variety of improvements, many of which the RSA current solution has already been providing for the last 10 years. This not only validates the RSA strategy, but also our position for first-to-market support of the new protocol. With only a few enhancements to add, the RSA solution will be ready to meet the market timelines as they evolve.

Table 1 illustrates where the current RSA offering already meets 3DS 2.0 standards and where we need to add functionality.

Requirement	3-D Secure 1.0.2 Protocol	EMV 3-D Secure Protocol (3DS 2.0)	RSA AAeComm 3DS 1.0.2 Offering
Frictionless user experience	X	√	√
Risk-based driven	X	√	√
Consumer enrollment excluded	X	√	√
Static password elimination	X	√	√
Mobile app coverage	X	√	X
ID&V and e-wallet support	X	√	X

Table 1: 3DS 2.0 Requirements vs. RSA Existing ACS, "Adaptive Authentication for eCommerce" (AAeComm)

Benefits from your participation in the new protocol

3DS 2.0 puts 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.

However serious fraud gets, genuine transactions will always vastly outnumber fraudulent ones. 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
- Data-rich authentication
- Cross-channel, device-agnostic support
- Smarter, broader authentication
- Faster all-around performance

The 3DS 2.0 protocol is data-rich because it adds dozens of new data elements to the communication flow. This new data will be passed from the merchants through the 3DS 2.0 network to RSA. Receiving more data means RSA will have more information to analyze, which we believe will take our industry-leading risk engine to an even higher level.

Smarter, broader authentication translates to a frictionless shopping experience for the majority of online consumers, who may not even realize that the RSA risk engine is protecting them in the background. Not challenging good customers (i.e., providing a frictionless shopping experience) is one of the main drivers behind the new protocol.

The changes coming with 3DS 2.0 lead to key benefits above and beyond the incredible results that the RSA solution is already providing.

You can achieve the following benefits from adopting the newer version of the protocol:

- More “top-of-wallet” loyalty from customers, as even fewer good sales are interrupted
- Higher overall approval rates for online transactions
- Mobile application and IoT device support for cardholders
- Even better fraud prevention, leading to reduced operational costs
- Richer data from merchants, allowing for a deeper view into consumer purchases

In today’s competitive consumer landscape, loyalty is largely channel-independent. Customer opinions can be shaped in a negative or positive manner in channels where issuers/processors have limited visibility or control. This is especially evident in mobile transactions, where the current 3-D Secure protocol is used sparingly. 3DS 2.0 opens visibility across channels, providing more control over consumer shopping and behavior. This provides issuers/processors with a more direct link to their customers, which empowers them to influence behavior and increase brand loyalty.

What we know today from EMVCo and the card networks

EMVCo first released the core specifications for the new 3-D Secure protocol in October 2016. At the time of release, the protocol was titled “EMV 3-D Secure 2.0.” Version 2.0.1 followed in June 2017, incorporating some market feedback and other changes, at which point EMVCo abandoned the versioning in the title and simply called the protocol “EMV 3-D Secure.” As of October 2017, the protocol had advanced to version 2.1.0. Naming nomenclature that includes a version number and shorter abbreviations tends to stick with people, so you will hear many people in the industry still refer to the protocol as “3-D Secure 2.0,” or simply “3DS 2.0.”

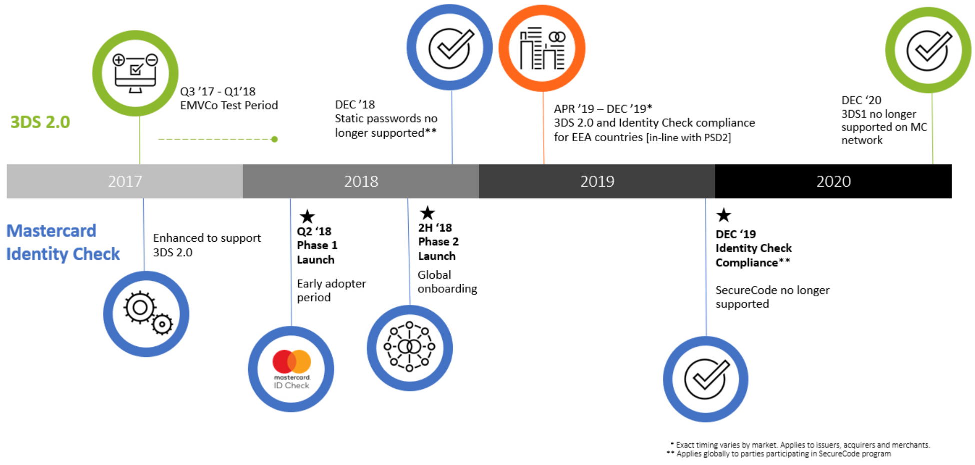
With the core specifications published, the certification process is the major remaining component. EMVCo originally planned to allow issuers to certify for the new protocol in Q4 2017, but this was eventually pushed to August 2018.

The card networks have issued various announcements over the last few years that tie back to inclusions in the new 3-D Secure protocol, such as timelines regarding the elimination of static passwords. As each card network publishes updated rules for incorporation of the 3DS 2.0 protocol, RSA will incorporate these into its ACS solution. This will assist issuers/processors with meeting the different program requirements.

In the meantime, see Figures 3 and 4 below for timelines that illustrate the EMVCo and card network milestones of which we are currently aware. Keep in mind that these dates are subject to change, like what we have seen with the EMVCo specification timeline. RSA recommends that you communicate directly with your card network representatives as you prepare to follow their new programs, so you can be sure you have the most up-to-date information.

MASTERCARD TIMELINE

Migrating from SecureCode/3DS1 to Identity Check/3DS 2.0

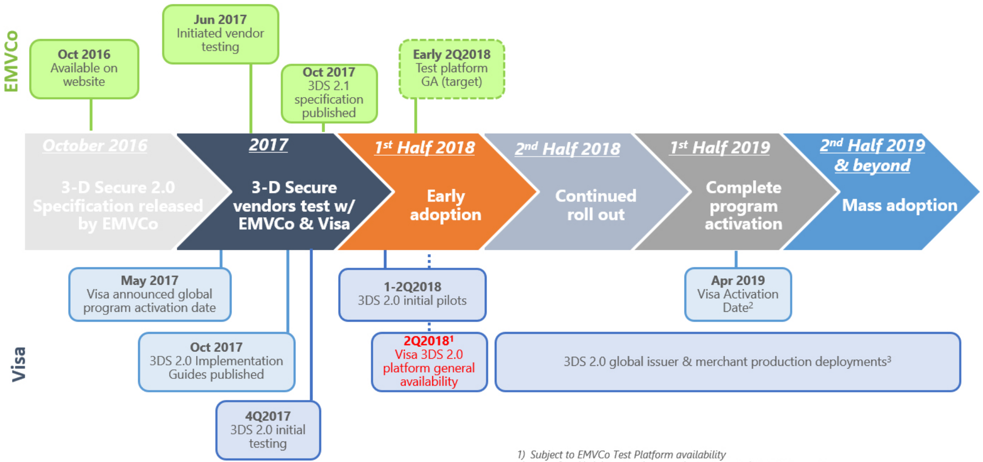

3DS 2.0
Q3 '17 - Q1'18
EMVCo Test Period
DEC '18
Static passwords no longer supported**
APR '19 – DEC '19*
3DS 2.0 and Identity Check compliance for EEA countries [in-line with PSD2]
DEC '20
3DS1 no longer supported on MC network
2017
2018
2019
2020
Mastercard Identity Check
Enhanced to support 3DS 2.0
★
Q2 '18
Phase 1
Launch
Early adopter period
mastercard
ID Check
★
2H '18
Phase 2
Launch
Global onboarding
★
DEC '19
Identity Check Compliance**
SecureCode no longer supported

* Exact timing varies by market. Applies to issuers, acquirers and merchants.
** Applies globally to parties participating in SecureCode program

Figure 3: Mastercard 3DS 2.0 (Identity Check) Timeline

VISA TIMELINE

Migration to 3-D Secure 2.0


EMVCo
Oct 2016
Available on website
Jun 2017
Initiated vendor testing
Oct 2017
3DS 2.1 specification published
Early 2Q2018
Test platform GA (target)
October 2016
3-D Secure 2.0 Specification released by EMVCo
2017
3-D Secure vendors test w/ EMVCo & Visa
1st Half 2018
Early adoption
2nd Half 2018
Continued roll out
1st Half 2019
Complete program activation
2nd Half 2019 & beyond
Mass adoption
Visa
May 2017
Visa announced global program activation date
Oct 2017
3DS 2.0 Implementation Guides published
4Q2017
3DS 2.0 initial testing
1-2Q2018
3DS 2.0 initial pilots
2Q2018[1]
Visa 3DS 2.0 platform general availability
Apr 2019
Visa Activation Date[2]
3DS 2.0 global issuer & merchant production deployments[3]

1) *Subject to EMVCo Test Platform availability*
2) *Issuer fraud liability extends to merchant-attempted 3DS 2.0 transactions*
3) *Based on existing EMV 3DS specification and functionality, version 3DS 2.1.0*

Figure 4: Visa and EMVCo 3DS 2.0 Timeline

Timeline for RSA

As a long-term advisor, RSA works closely with both EMVCo and the card networks. You can expect a phased rollout approach from us. Our current release offers support for early adopters and protocol tests, and will be followed by releases that contain incremental functionality. As the individual card networks release their 3DS 2.0 programs, RSA will certify with those programs to fully enable our customers. Look for further communication from RSA as we move forward with our development and release timeline.

What you need to do to prepare

As an issuer/processor, you should consider the following so you can participate in 3DS 2.0:

- Identify the card programs you'll be supporting (e.g., Verified by Visa, Mastercard Identity Check, etc.) and assure your go-to-market plans are aligned with them. You can review this with your assigned card brand representative(s).
- Open projects with the relevant card brands that you issue. As they publish the final versions of their 3DS 2.0 programs, you will want to follow the program instructions to onboard your card portfolios to the 3DS 2.0 platform.
- Set up a process to provide RSA with your chargeback data. Note that if you are an existing RSA customer, you may already be doing this. You can work with your RSA Professional Services representative to arrange this.
- Ensure the key exchange/loading process is set up for each card brand you issue. For Visa, your existing keys will work for 3DS 2.0. Mastercard will not require keys. If you have questions or need help regarding keys, we encourage you to work with your RSA Professional Services representative.
- Test 3DS 2.0 traffic with each card network you support.
- Load the appropriate BIN ranges with RSA and each card network. The card networks are provisioning new 3DS 2.0 Directory Servers, and will keep the existing 3DS 1.0.2 Directory Servers separately running in parallel. You will need to upload your relevant portfolios to the new 3DS 2.0 servers, even if your current participating BINs are already loaded into the card network 3DS 1.0.2 servers.
- Go live with 3DS 2.0 traffic! Keep in mind that for a time you will be running both 3DS 1.02 and 2.0 traffic in parallel with RSA. Over time, as merchants continue to adopt the new protocol and each card brand phases out the 1.02 protocol, the traffic will consolidate into 3DS 2.0 only.

Additional things to keep in mind:

- You need to be certified with EMVCo. Note that if you select an EMVCo certified vendor, such as RSA, it will eliminate the need for you to get your own certification. EMVCo has published its certification specifications, which you may reference on their website.
- Keep in mind that a major component of 3DS 2.0 is to eliminate static data, such as passwords, from the authentication process and to only challenge consumers if a transaction appears to be risky (i.e., dynamic,

risk-based authentication). RSA recommends you assess your current authentication methodology in preparation for a dynamic, risk-based authentication environment.

- As a part of this assessment, if you don't already do so as part of an existing routine, you should plan on vetting your customer contact information in preparation to handle these new, dynamic authentication methods. This may include verifying the accuracy of customer mobile numbers, email addresses, and similar contact information—or asking your customers for them to begin with, if you don't already have them on file.

Frequently asked questions

Here are some common questions and answers to consider as you move toward implementing the new program:

When do we have to be ready for 3DS 2.0?

This will depend on what the various card networks announce regarding their individual programs, and which type of cards you issue. For example, if you are a Visa issuer, you will note that Visa has announced when issuers within various regions must stop using static data elements (such as passwords). Of course, not using static data elements is one of the requirements in the new 3-D Secure protocol, so this will bring participating issuers closer to 3DS 2.0 readiness. Visa has also announced that by Q2 2019 issuers in all regions must be completely 3DS 2.0-ready, but we are likely to see different timelines for each geographic region. You can refer to Figures 3 and 4 to see what we know today about the timelines and cutoffs. No matter the timing of each card brand's program, one thing remains sure—you don't want to be caught unprepared when merchants start sending 3DS 2.0 traffic. This is one reason RSA highly recommends getting ready now, rather than waiting for the traffic to come.

How do we manage both kinds of 3-D Secure traffic at the same time, and how will we know which is which?

Until the existing 3-D Secure protocol is terminated by the various card networks, traffic from both the existing and new protocols will be flowing between merchants and issuers. RSA will route both kinds of traffic appropriately through a single ACS connection, and there will be no need to utilize two separate instances of the ACS to facilitate both kinds of traffic. RSA will indicate which transactions came in as 3DS 1.02 and which came in as 3DS 2.0. As the old traffic tapers off (and is eventually terminated) and the new traffic continues, the transition will be seamless for your business.

What should we do with the new data elements?

You may have heard that 3DS 2.0 introduces dozens of new data elements associated with each payment authentication request. These new data elements are defined in EMVCo's specifications. RSA will be using the new data to further enhance our risk engine and make even better risk assessments and recommendations for your organization—but your internal business teams could also gain a lot of critical insights that were previously unavailable.

What have you heard about the plans for merchants to adopt?

This is a common question we hear from issuers and issuing processors. We know that both parties (issuers and merchants) need to adopt the program for it to be truly beneficial, and each party wants to know that the other will be adopting! RSA recently conducted a merchant survey, asking about 150 top-tier online merchants a number of 3-D Secure-related questions, including their plans to adopt. Almost 60% of merchants surveyed indicated they are planning to adopt the new program. Javelin Strategy recently conducted a similar survey with a broader participation base, and found that about 44% of surveyed merchants are using the current 3-D Secure protocol and plan to adopt the new one, while 19% of those who have never used 3-D Secure plan on implementing the new protocol as it rolls forward (a total adoption rate of 63%). Although we're still in the early stages of the new protocol, these responses show us that a critical mass of merchants is already forming. We anticipate the number of merchants planning to adopt to grow further, as RSA and other organizations (such as the major card brands) continue to educate the industry about the benefits of participation.

What authentication options should we consider to comply with the dynamic vs. static data element requirements from the card brands, as well as in the 3DS 2.0 protocol?

You will have the same authentication choices with 3DS 2.0 that you have with the current offering by RSA, but you will want to avoid options that utilize static data elements (such as passwords or set questions/answers), as these will no longer be allowed. Instead, you will want to focus on methods that are dynamic or qualify as strong customer authentication. Such methods include technologies like biometrics, one-time-passwords (OTP) or other types of multi-factor authentication. If you are already using effective versions of these services and technologies today, you can continue to use them for 3DS 2.0 transactions.

Can we participate in an early adopter or testing process of some kind?

Yes. When the card networks and EMVCo processes are ready, RSA will be happy to support customer pilots. These pilot implementations will be based on RSA availability and provided on a first-come, first-served basis. Contact your RSA Professional Services representative if you'd like to hear more about your participation options.

How RSA global services can help

RSA Global Services helps customers get the most out of their RSA products. We can help facilitate your journey to 3DS 2.0, whether you are an existing RSA customer or are considering one of our solutions.

Optimizing your 3-D Secure 2.0 onboarding

If you are an existing RSA Adaptive Authentication for eCommerce customer, implementation specialists from our Professional Services team will review the processes, screens and other elements in your existing 3DS 1.0 environment and help you determine whether these should be augmented to support a 3-D Secure 2.0 implementation. Rather than augment your existing deployment, you may opt to consult with our implementation specialists to design a new implementation “from scratch” to best leverage the enhanced cardholder experience promised by 3D Secure 2.0. If you are not an existing Adaptive Authentication for eCommerce customer, our Professional Services team can help you prepare to onboard once the card networks have prepared their 3-D Secure 2.0 programs.

Additional value-added services

In addition to implementation specialists, RSA Professional Services offers a range of value=added services that can help make your journey to 3-D Secure 2.0—as well as the ongoing operation of RSA Adaptive Authentication for eCommerce—as productive, effective and efficient as possible.

RSA Risk Account Managers

Our Risk Account Managers (RAMs) can help optimize your RSA Adaptive Authentication for eCommerce deployment from a fraud and risk-management perspective. They will analyze trends across fraud detection, challenge and failure rates (for example), and provide guidance to improve performance. They will also work with you to deploy rules in the Policy Manager that enable you to get the most from the new protocol. This veteran team understands the fraud landscape, the 3-D Secure 2.0 protocol and the product. RAMs can provide expert advice for achieving your fraud-detection goals while maintaining a frictionless cardholder experience.

RSA Service Account Managers

Our Service Account Managers (SAMs) provide a concierge-like service. They orchestrate all post-sales issues and activities and act as a single point of contact for all business and technical issues. The SAMs work closely with the RAMs, as well as our Product, Engineering, SaaS Ops, Finance, Governance Risk and Compliance, Education Services, and other teams to manage the resolution of all your technical and business queries (whether they are related to 3-D Secure 2.0 or not). The SAMs ensure that each interaction you have with RSA is efficient, collaborative and productive.

About RSA

RSA® Business-Driven Security™ solutions link business context with security incidents to help organizations manage digital risk and protect what matters most. With award-winning cybersecurity solutions from RSA, a Dell Technologies business, organizations can detect and respond to advanced attacks; manage user identities and access; and reduce business risk, fraud and cybercrime. RSA solutions protect millions of users around the world and help more than 90 percent of Fortune 500 companies take command of their security posture and thrive in an uncertain, high-risk world. For more information, visit rsa.com.

RSA