fime

A guide to EMV® 3-D secure

Fighting fraud & friction in online payments.

December 2019

fime.com

Contents

1. Introduction.

We’re all paying, transacting and managing our financial lives in an increasingly online and digital world.
This has driven a new age of consumer convenience but in parallel, a new age of fraud.

Fraud, as always, migrates to the weakest point. And the physical payments world has strengthened security in recent years.

With EMV®[1] chip card adoption gathering momentum globally too, fraudsters have found the digital world of card not present (CNP) transactions the easiest to exploit.

1 EMV® is a registered trademark in the U.S. and other countries and an unregistered trademark elsewhere. The EMV trademark is owned by EMVCo, LLC

The stats speak for themselves!

Whether e-commerce, m-commerce or remote commerce...

It's estimated that digital fraud rates now account for 60-70% of all card fraud in many developed countries[2].

It was even estimated that the gains made from savings in card-present fraud were eclipsed in 2018 by the losses from CNP fraud[3].

2 https://www.experian.com/assets/decision-analytics/white-papers/juniper-research-online-payment-fraud-wp-2016.pdf

3 https://www.pymnts.com/news/2015/outsmarting-the-cnp-fraudsters/

The market responded with measures to overcome the challenges of online fraud. But many added too much friction.

At odds with the ‘age of convenience’, consumers have responded negatively to existing **authentication methods**, such as complex static passwords to remember.

And it’s harming retailers too.

Approval rates for digital transactions have dropped significantly. The eCommerce cart abandonment rate is at nearly 70%.

And, around 28%[4] of U.S. online shoppers admit to quitting orders due to checkout processes being too long or complicated.

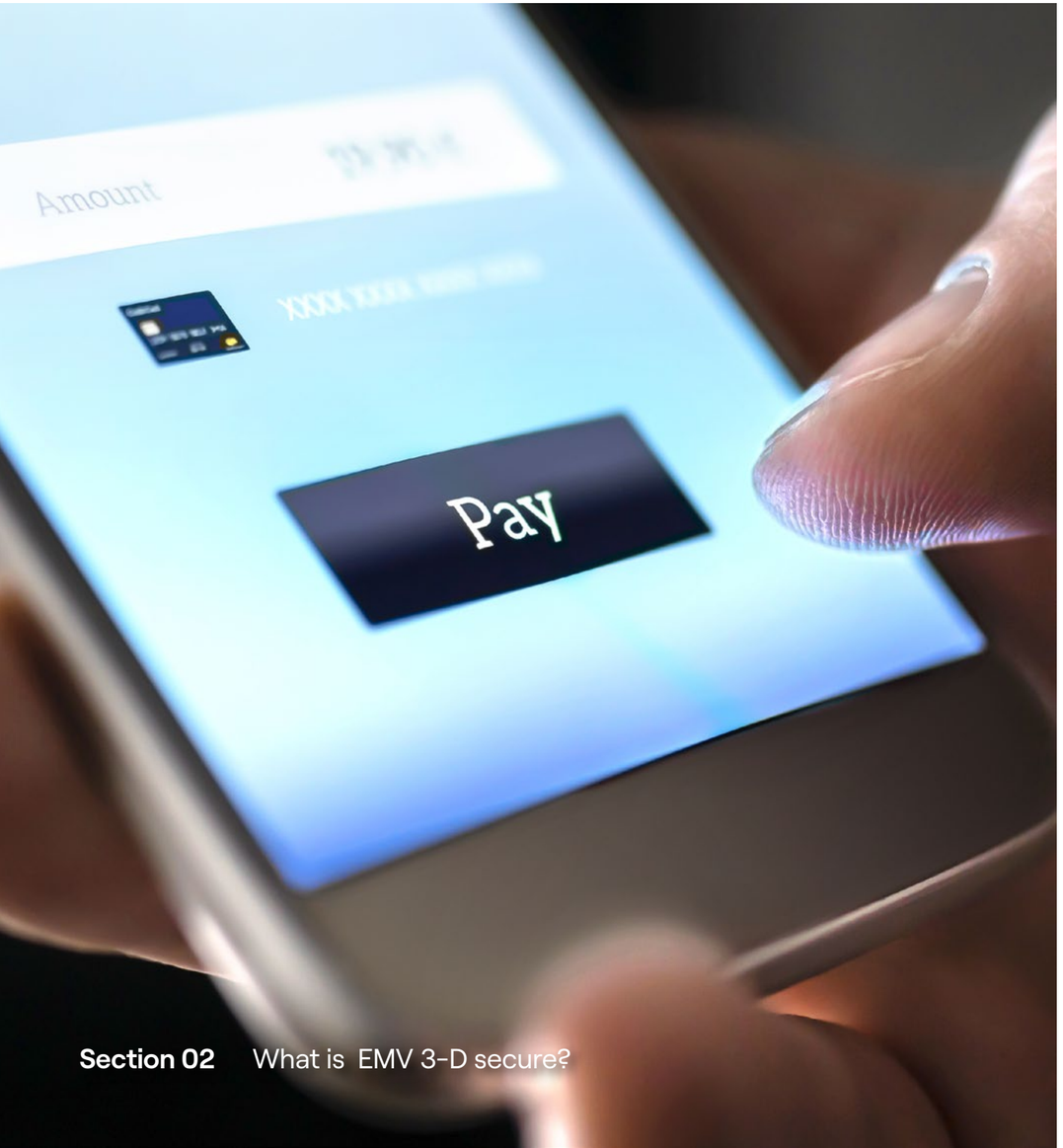
4 "41 Cart Abandonment Rate Statistics", Baymard Institute (September 2019)

The online world is playing catch-up to achieve a similarly harmonized, secure authentication solution as the physical world, while improving the UX.

EMV 3-D Secure (or EMV 3DS) is one solution that's leading the way in the CNP 'catch up'.

But what is EMV 3DS? And why is it important for the future of CNP payments?

2. What is EMV 3-D secure?



Three-Domain Secure (3DS) is a standard messaging protocol used to authenticate cardholders for CNP transactions.

It defines a standardized, harmonized and secure authentication solution for all stakeholders: merchants, issuers, acquirers and payment networks (commonly referred to as payment schemes).

In short, it aims to offer a frictionless online authentication solution.

The first version was initiated by Visa and was quickly followed by other international payment schemes. This was a fragmented and complex solution for the industry.

Now, industry body EMVCo has taken ownership and is managing the evolution of the specifications.

3. Bridging the gaps.

The original implementations worked to address the following 3 points with varying success:

- Increase approval rates
- Reduce fraud
- Enhance the user-experience

Increase approval rates.

Driving up the total volume of transactions is the bottom line for retailers, banks and schemes alike.

Boosting these is fundamental to EMV 3DS, and these transactions generally see 10–11% higher authorization rates than non-3DS transactions[5].

On the other hand, this also helps remedy the losses and resulting customer dissatisfaction of false declines.

5 "3-D Secure 2.0: Key Considerations for Merchants", Aite Group (October 2018)

Reduce fraud.

By championing a risk-based authentication approach, EMV 3DS is helping reduce fraud, saving issuers money and creating more confident consumers.

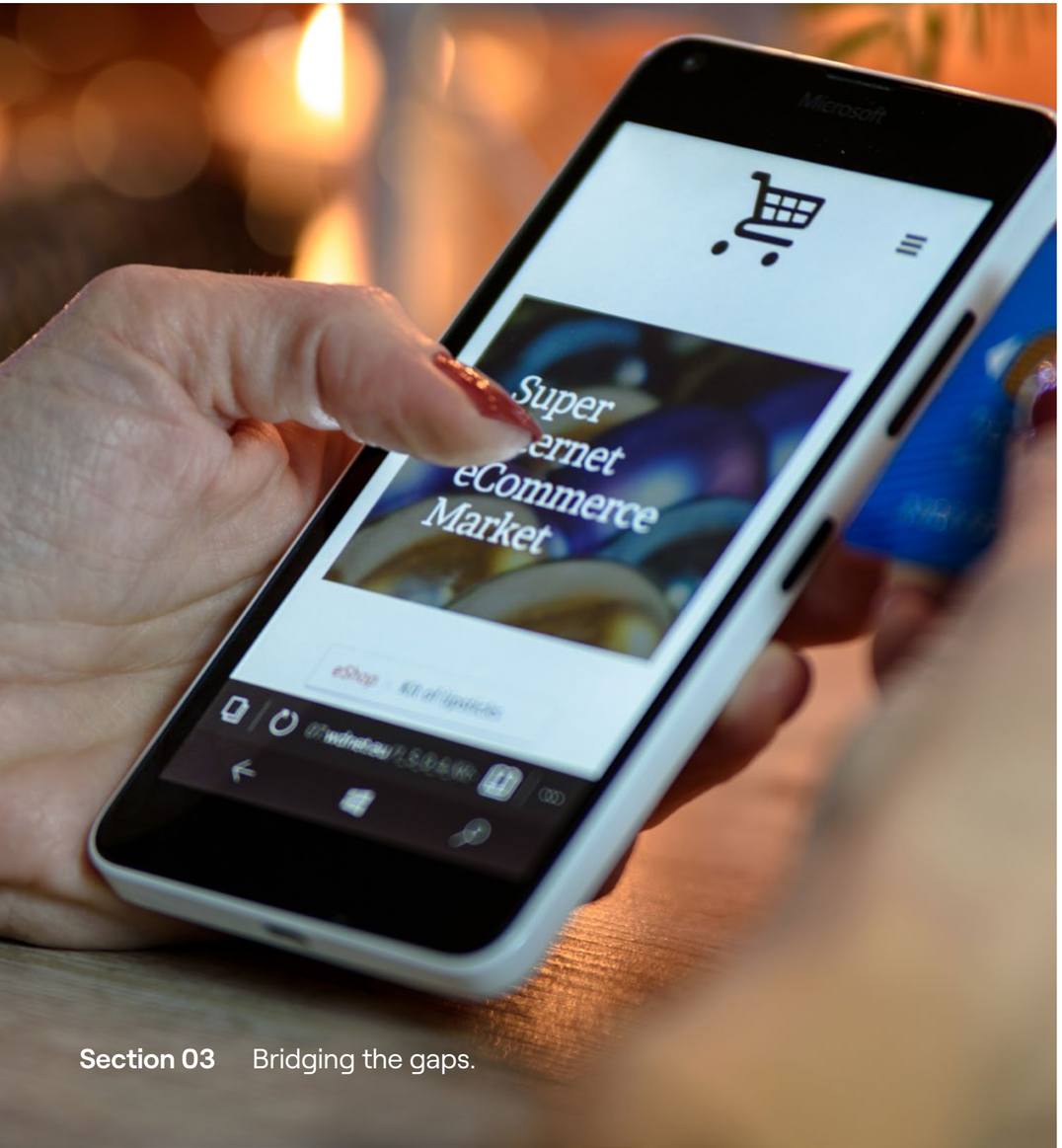
Historically, the liability of fraudulent chargebacks has sat with merchants or issuing banks.

But, with EMV 3DS, responsibility is shifting depending on which version of 3DS is supported during the authentication, meaning retailers especially can benefit.

Enhance the user experience.

Remembering the 3rd, 5th and 8th digit of a password set five years ago is not a very friendly user experience.

In addition, limited support for different devices, channels and authentication methods was forcing the consumer to redirect between different webpages or apps.



Eradicating these complex additional steps and points of friction is vital to reducing cart abandonment and driving sales for retailers.

Not to mention making happier customers keen to return!

What’s new?

The latest version of the EMV 3DS specifications fundamentally realizes these objectives by **improving communications** ‘in the background’ between the issuing bank, the acquirer and the merchant.

Rather than requesting information from the user, basic account holder information is now automatically retrieved and verified.

And smarter algorithms are in place to ensure requests for further authentication are made only when really needed.

To give some context of the upgrade, the enhanced data stream in the latest version has increased from sharing 15 data fields, to over 150[6].

Let's take a closer look at some of the new features:

- More authentication options
- Multiple platforms and digital channels
- Non-payment categories
- Alignment with regulatory requirements
- More choice

6 "3-D Secure 2.0: Key Considerations for Merchants", Aite Group (October 2018)

More authentication options.

Replacing ineffective static passwords with more complex authenticators including dynamic one-time passwords and biometrics, such as facial recognition and fingerprint, where available.

Multiple platforms and digital channels.

Enabling support for in-app, mobile browser and digital wallet services, in addition to traditional browser applications.

The latest EMV 3DS specifications support symmetrical authentication flows[7] across applications and browsers.

Integration across environments is simplified and cardholders receive a consistent buying authentication experience irrespective of platform.

7 "An update on EMV 3-D Secure webcast", EMVCo (August 2019) https://www.youtube.com/watch?v=7_4fOqJfPmk&feature=youtu.be

Non-payment categories.

Supporting identification and verification applications as well as payments.

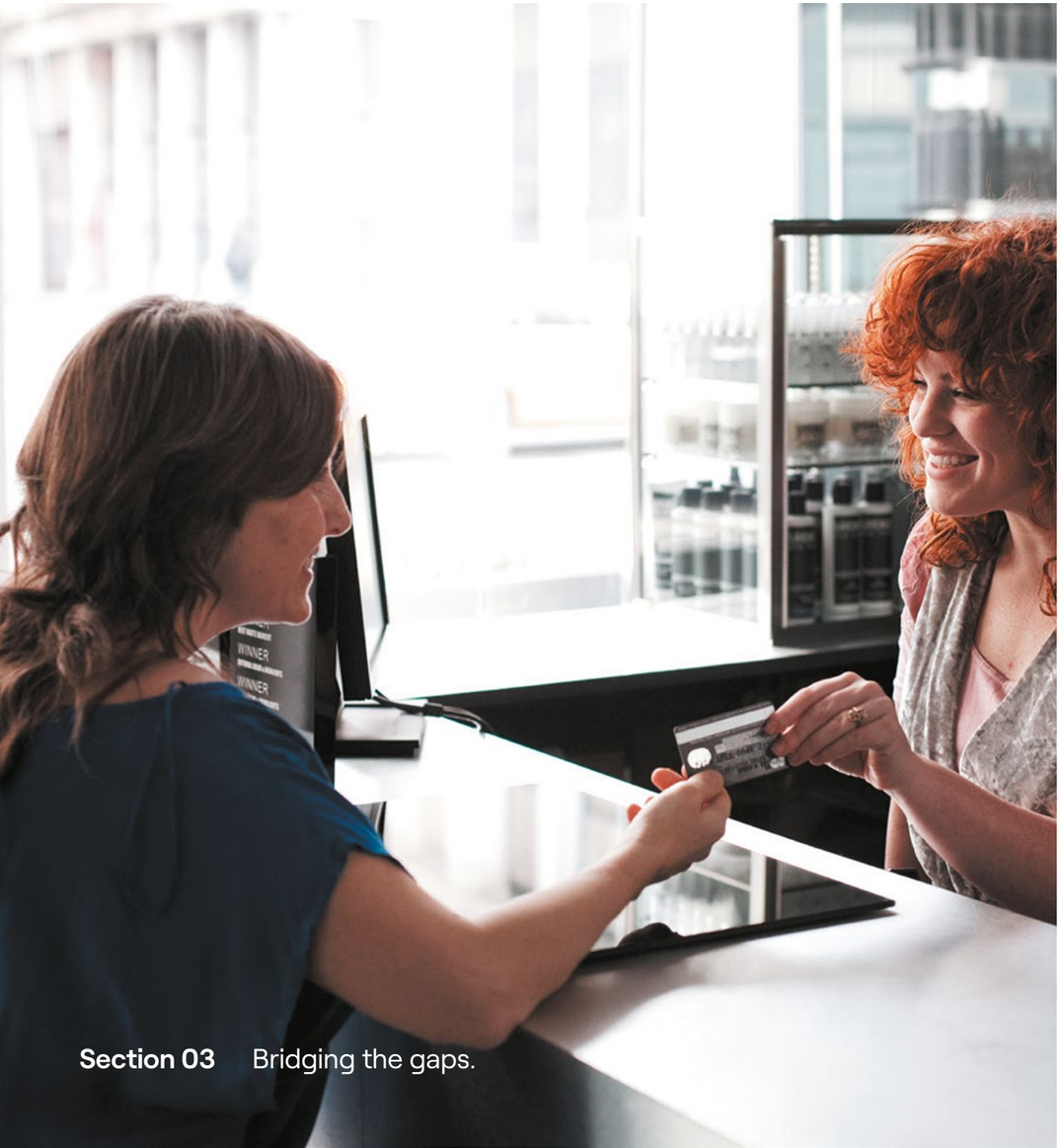
While the use cases are still being explored and defined, these could include adding a new payment card to a mobile wallet, opening a new account online, or governments utilizing it to authenticate citizens.

With more data included in the message requests, indications such as whether Acquirer SCA or a transactional risk analysis (TRA) have already been performed, or if a customer utilized a FIDO authenticator, can simplify the authentication process.

More choice.

Enabling customers and merchants to have greater input. A feature of the latest version of EMV 3DS enables customers to ‘whitelist’ merchants with their issuer when setting up, say, a recurring purchase.

This lets banks know a full review is not required, reduces customer prompts and can help support banks in risk ‘scoring’ merchants.



Another feature gives merchants the option to implement a non-challenge mode, feeding the results of EMV 3DS into their risk analysis and approve / decline decisions.

EMV 3DS in practice. This is an example.

The cardholder is on holiday in another continent, making an m-commerce transaction from a retailer that's never been used before.

These parameters would trigger the bank to request one of the new authentication modalities such as:

- A biometric authentication
- Out-of-Band authentication completed outside of 3DS
- One-Time Passcode (OTP)

4. The EMV 3DS chain. Who’s involved?

The 3-pronged infrastructure (hence the name) remains largely unchanged from original EMV 3DS implementations.

The protocol links the financial authorization process with the online authentication, usually via a popup window prompting the user to input additional authentication.

The players involved can be understood in the diagram coming next, page 32.

ACS
Access Control Server

The issuer’s server of the card in use, who is responsible for authentication of the cardholder.

3DSS
3DS Server

The communication between the merchant environment initiating authentication request and the DS to send and receive authentication messages.

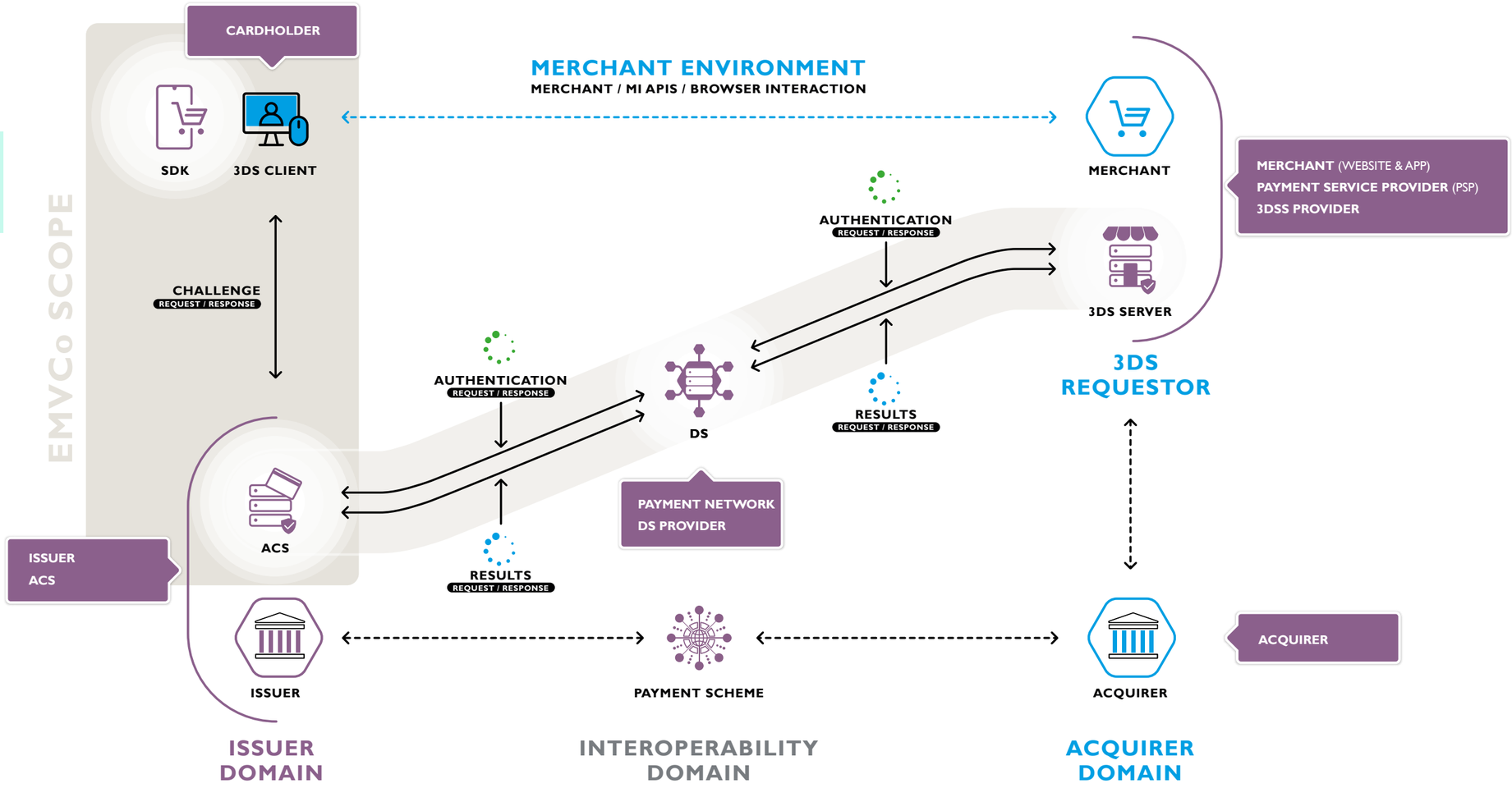
DS
Directory Server

This central domain is operated by each participating payment networks.

Merchant APP 3DS SDK

The Software Development Kit (SDK) running on the consumer device for in-app purchases, communicates with the 3DS Requestor Environment and ACS in case of additional authentication information requested.

Stakeholders in the 3DS ecosystem



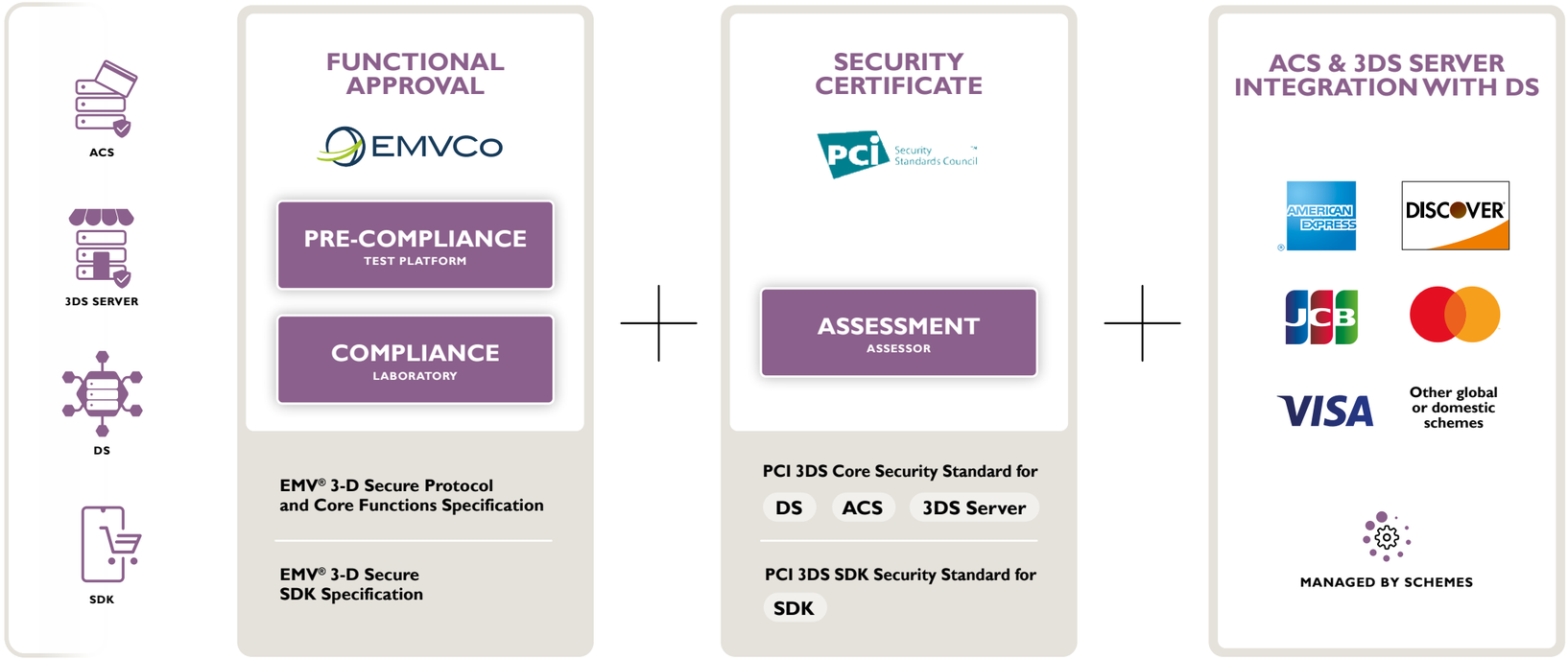
Note: dashed arrows and merchant server are not part of 3DS and are shown for clarity only.

5. Defining your requirements.

Wherever in the online payments chain you sit, EMV 3DS is a compelling authentication solution fit for the digital, omnichannel age.

But implementation does not come without its challenges and testing requirements.

Before embarking on an EMV 3DS project, **there are 3 key stages of testing to consider** whether an entirely new system or upgrading a legacy system.



1. Functional.

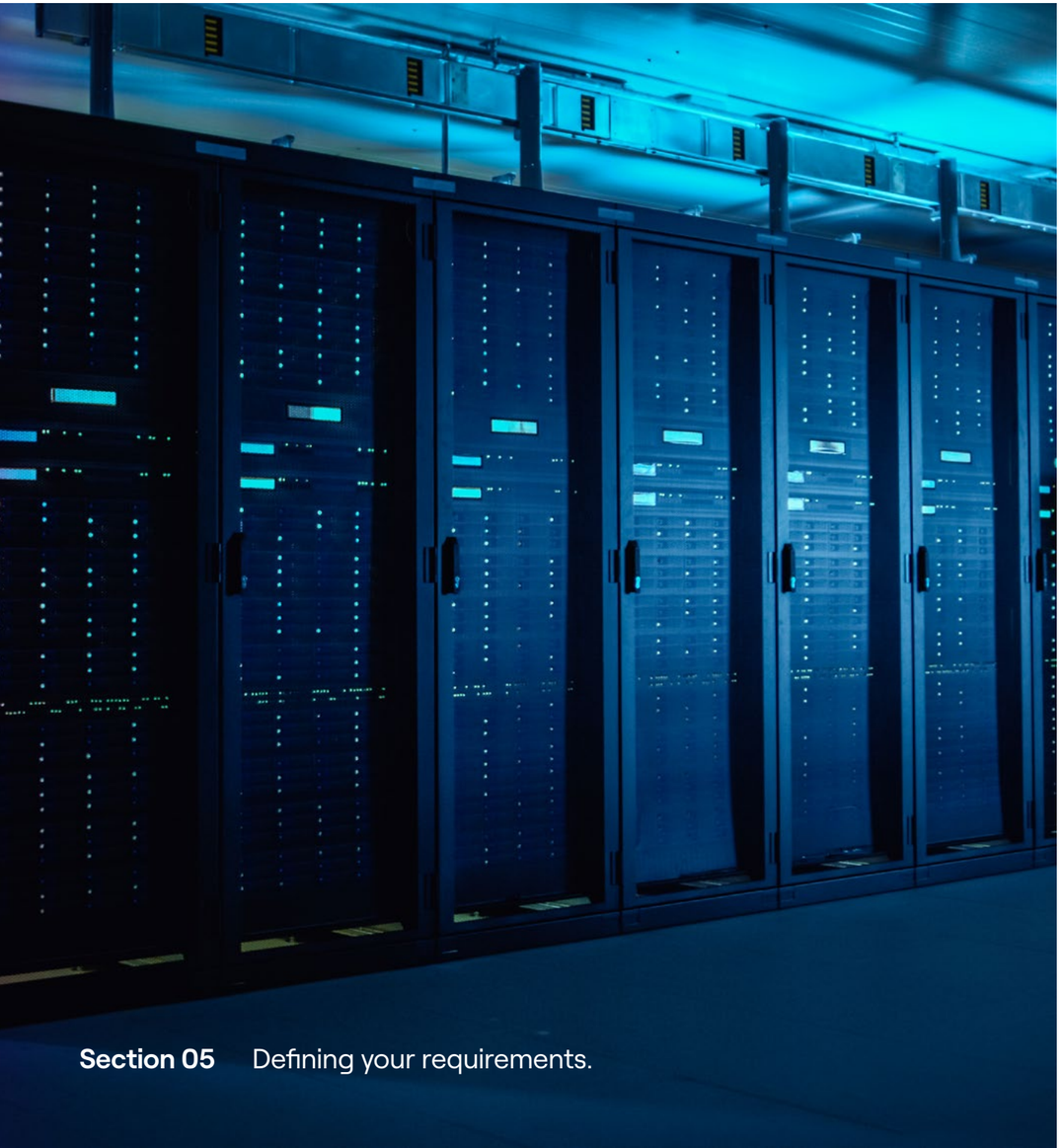
This initial functional testing is defined by EMVCo.

It incorporates pre-compliance and compliance testing to align with the EMV 3-D Secure Protocol and Core Functions Specification, and the 3-D Secure SDK Specification.

ACS, 3DS Servers, DS and SDK providers all fall under scope here.

2. Security certificate.

The security layer of testing is managed by PCI SSC and is applicable to the payment networks, the ACS and the 3DS Server. PCI also has a 3DS SDK Security Standard for SDK providers.



3. ACS & 3DS Server Integration with DS.

In addition to functional and security testing, payment schemes have initiated their own integration standards for ACS and 3DS servers to ensure the compliancy of their customized implementation requests between the server providers, issuers and acquirers.

Onboarding and integrating effectively with each chosen scheme’s Directory Server is a key final step ahead of launch.

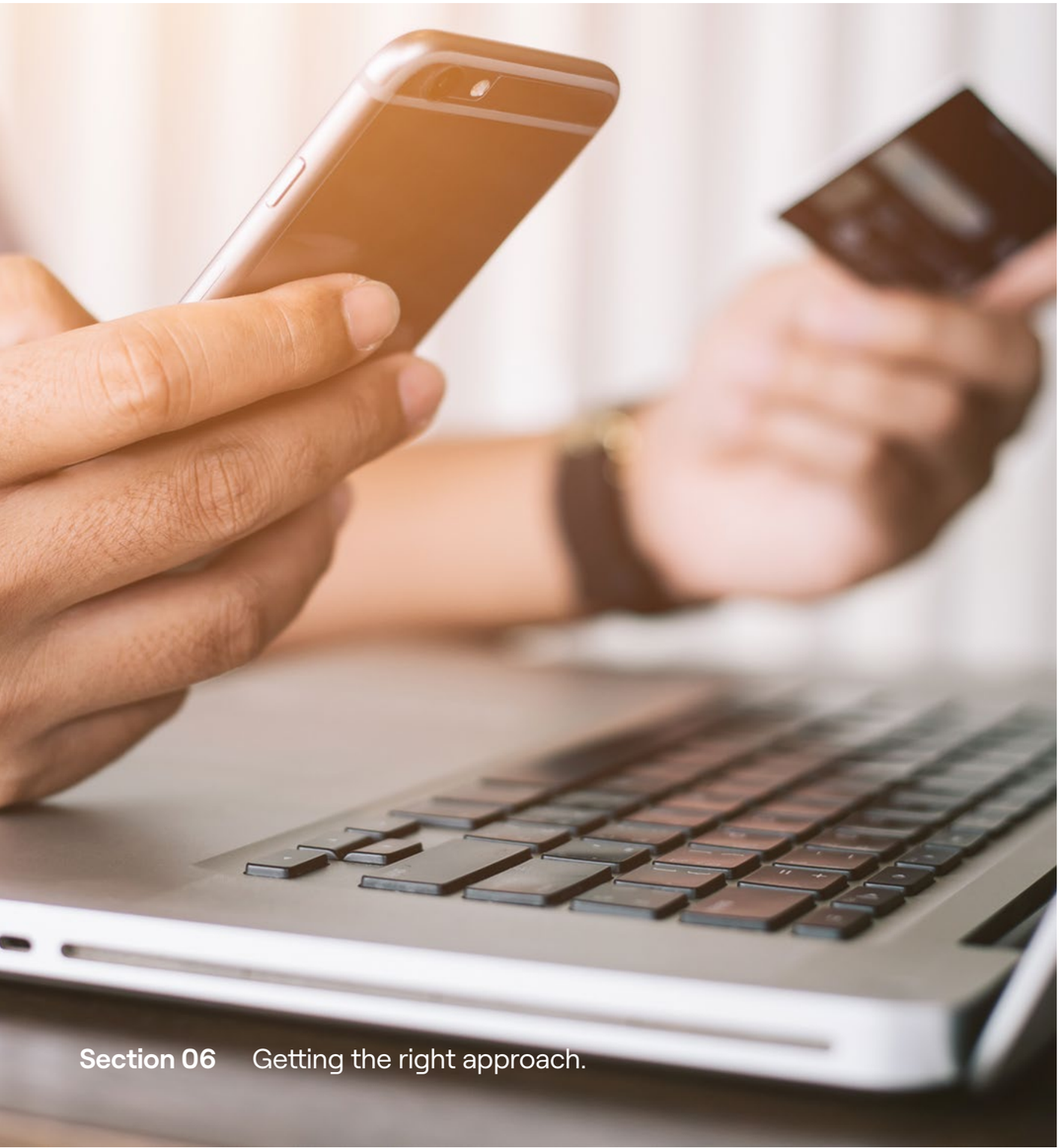
6. Getting the right approach.

Understanding what scope of testing falls to each stakeholder and navigating the three stages quickly and cost-effectively can be a challenge.

And it’s here where support from a reliable testing and consulting expert on EMV 3DS can be invaluable.

2.1 or 2.2?

Throughout this eBook, we've spoken generally about the latest EMV 3DS specifications. But you may have requirements for features specific to the very latest version of EMVCo's protocol, 2.2.

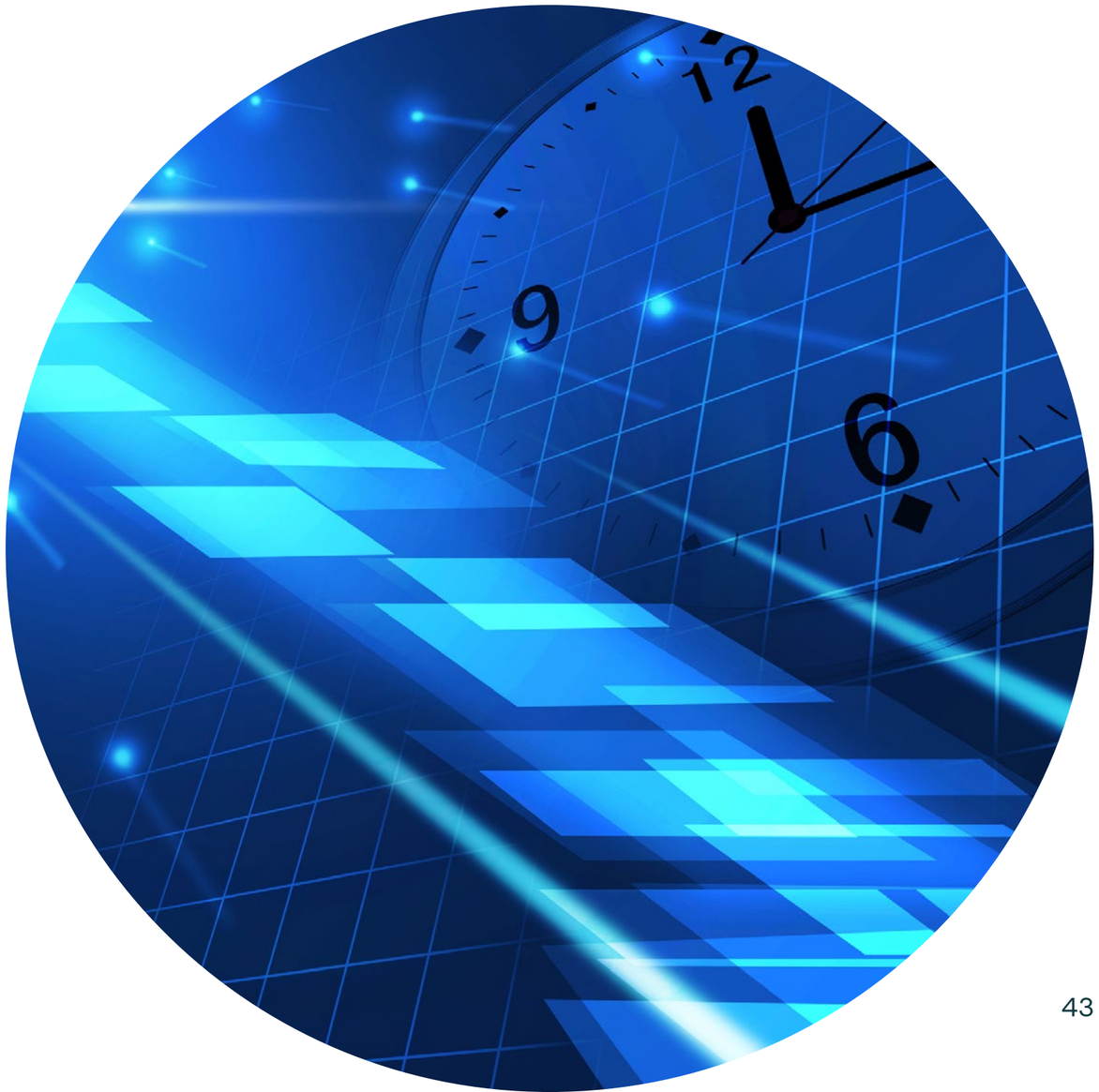


Deciding which version of the protocol to implement can be challenging. 2.2. offers a few valuable new features such as:

- Whitelisting
- Acquirer exemptions
- Support for new data streams from the relying party
- New authentication channels

However, 2.1 has a more mature test platform, with fewer features to be tested at EMV-level, reducing the time and complexity to compliance and launch.

An expert in the nuances of EMV 3DS can help balance the factors and decide the solution most valuable to your market.



With competing timelines for payment network liability shift and migration policies, and PSD2 SCA running in parallel, plotting out an effective comprehensive test plan will ensure your project stays on time and on budget.

In conjunction, effective testing and issue analysis support needs to be in place throughout to ensure projects maintain momentum.

It’s also worth noting that 3DS itself is no silver bullet, and there are several other factors to consider to ensure an effective online transaction risk assessment process is in place.

A consultant with a broader view of the payments ecosystem can ensure the bigger picture is taken into account from the start of projects.

7. Fime solution.

Fime’s long history supporting the industry’s digital transformation and long-standing participation in EMVCo enable us to deliver unrivalled expert support for your projects.

Our unique offering combines testing support with consultancy expertise.

With over 20 years' as a trusted third-party testing partner in payments testing, Fime has defined a market-leading test platform.

Our automated, cloud-based test tool can empower regular testing from any location and at any stage of your project. The platform champions a user-friendly approach, enabling you to remain agile, reviewing and resolving issues quickly and efficiently on the path to product launch.

In addition to the DIY tool, Fime's dedicated expert team is also on-hand to support issue analysis.

We support testing for the four modules composing the three domains of a 3D-Secure ecosystem: ACS, 3DSS, SDK and DS.

Combined with a full package of security services, delivered via our trusted partners, and tailored consultancy services, Fime delivers truly end-to-end project support.

Get in touch today to start your migration to EMV 3DS. Learn more about Fime user-friendly 3DS testing services here.

Defining the needs and objectives of 3DS implementation

Business & technical analysis

- Business & regulation impacts
- Specific requirements gathering / writing / audit
  - How and which ACS to implement (issuers)
  - How and which 3DSS to implement (service providers)
  - How to manage the integration with the different DS from the schemes
- 3DS solution benchmark (DS, 3DS server, ACS)
- Support on RFP writing and bidders scoring
- Support choosing the correct strong authentication solution and management process for customers (issuers)

Implementation and migration project support

- Technical migration assessment
- Technical migration support
- Define the specific requirements for the DS (schemes) including problem management
- Define the business rules test plan

Implementation and testing support

Test and certification process support

- Define the associated test methodology
- Workshop / custom test plan for domestic schemes for DS (additional layer)
- Realization of test plans
  - With the DS and with the 3DSS (issuers)
  - For the SDK tests for merchant APP 3DS with the DS, and the merchants (service providers)
- Setting up an ACS sandbox, including the integration testing with service providers (issuers)
- Implementation of a 3DSS sandbox to help merchants in their integration tests (service providers)

Trainings & workshops

Available on-demand

- 3DS overview
- 3DS 1.0.2 vs 2.0
- Testing & certification

Discover more about how Fime can help your business.

Making innovation possible.

To learn more about how
Fime can help your business:

visit fime.com

or contact sales@fime.com