SCA Managed Rollout Programme

3DS testing approach and guidance document

Contents

Background and purpose of this document

The UK Finance Strong Customer Authentication (SCA) Programme Management Office (PMO) established the Technical Working Group (TWG) to help provide input on technical issues in relation to the SCA Managed Rollout Programme.

The TWG identified a need to provide the wider industry with supplementary guidance on the testing they should consider in the technical implementation of 3DSecure (3DS) v2.X.

The UK Finance SCA PMO has therefore developed this document to support and provide high-level guidance to e-merchants and issuers.

The TWG recognises that business as usual (BAU) testing takes place at an individual business level when there is a payments-related technological upgrade. This document is not intended to replace BAU testing, but instead to supplement and provide guidance.

For the avoidance of doubt, reference to 3DS v2.X – includes both 3DS v2.1 **and** 3DS v2.2.

The UK Finance SCA PMO Implementation Task Force (ITF) is responsible for defining the detail of an industry-wide rollout of SCA. In July 2020, the ITF presented its proposed ramp up definition to the Financial Conduct Authority's SCA Monitoring Forum to avoid a cliff edge implementation of SCA within the UK.

For the UK only - the industry agreed the ramp up period for soft declines and step ups is **31 May 2021**. From 31 May 2021 issuers will begin to gradually increase soft declines and step ups of non-compliant transactions in the lead up to the FCA enforcement date of 14 September 2021. Therefore, the bulk of testing by participants should be completed before 31 May 2021.

Full details of the ITF's proposed implementation plan and SCA ramp up can be found here.

1. Testing overview & call to action

With the introduction of any technological upgrade across the payments industry, there is an established process for testing, accreditations, and certifications between participants in the payments value chain (BAU testing). The below diagram (*diagram 1*) shows, at a high level, some of the testing that takes place between participants in this process.

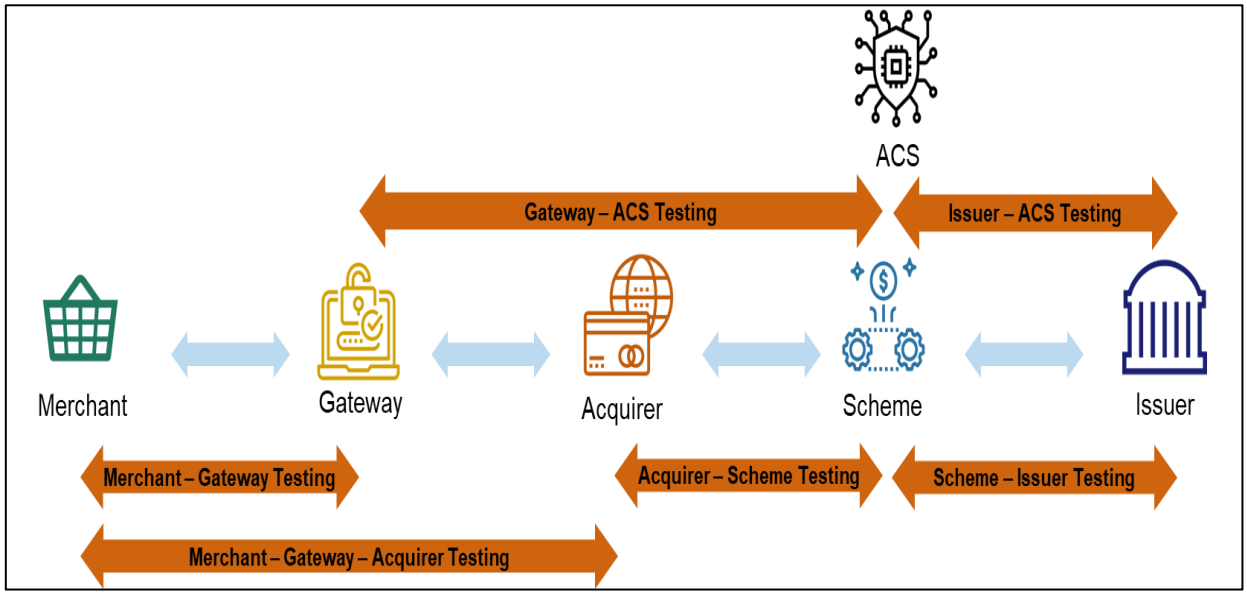

DIAGRAM 1

The TWG recognises there will be more testing that takes place as a matter of course that has not been identified in diagram 1. The purpose of the diagram is to highlight the numerous testing partnership interdependencies that are critical in ensuring that all technological upgrades, when they go live, do not severely impact customers or e-merchants.

Each participant is responsible for ensuring that they undertake adequate testing.

The testing outlined in diagram 1 ensures that all participants within the payments value chain can process transactions effectively i.e. technical implementation testing.

What is the industry is doing to provide supplementary testing support for 3DS implementation?

- **Card scheme led testing**

The three major UK schemes Visa, Mastercard and American Express have announced testing support in the form of:

- issuer self-testing / simulated e-merchant
- e-merchant self-testing
- acquirer self-testing
- end to end testing with top issuers and e-merchants in EEA countries to test 3DS frictionless and challenge flows.

- **TWG testing facilitation**

For a limited number of participants, the TWG will look to assist in the matching up of issuers and e-merchants to undertake end to end testing. Due to the risk and fraud concerns in relation to publicly issuing test primary account numbers (PAN) this is not a large-scale offering.

Call to action (market participants)

In the lead up to industry co-ordinated SCA ramp up commencing from 31 May 2021 and enforcement date of 14 September 2021, the UK Finance SCA PMO urges all participants in the payments value chain to begin and/or continue testing their 3DS implementation.

E-merchants

- Engage with your payment solution provider (gateway) and/or acquirer to implement your 3DS solution.
- Engage with your payment solution provider (gateway) and/or acquirer to undertake technical implementation testing to ensure your 3DS solution functions effectively and you have the required certifications and accreditations in place ahead of 31 May 2021 commencement of industry SCA ramp up period.
- Review test scenario use cases and identify and test those that are applicable to you (in the absence of test cards, e-merchants may look to use cards from other sources).
- Review and implement recommendations contained within 3DS optimal field completion guidance to decrease challenge rates on 3DS v2.X (located in appendix 2).
- Review and take on board the observations and learnings from TWG testing facilitation (located in appendix 3).

Gateways

- Engage with your entire e-merchant base as soon as practicable to communicate and discuss the forthcoming SCA regulation and how it will impact them and their customer base.
- Discuss with your e-merchant base the implications (soft declines and step ups) of an industry co-ordinated SCA ramp up period commencing from 31 May 2021.
- Ensure that there are plans to have implemented an SCA compliant solution for your e-merchant base with sufficient testing for each e-merchant. This is to help ensure their solution is implemented correctly ahead of the SCA ramp up period beginning from 31 May 2021.
- Engage with acquirers as soon as practicable to ensure that your organisation has the accreditations in place on the versions of 3DS well in advance of 31 May 2021.
- Review and implement recommendations contained within 3DS optimal field completion guidance with your e-merchant base to help support their transition onto 3DS v2.X (located in appendix 2).
- Review and take on board learnings and observations from TWG testing facilitation (located in appendix 3).

Issuers

- Ensure technical readiness for 3DS v2.X by 31 May 2021.
- Undertake testing of 3DS v2.X with numerous merchants in multiple merchant sectors ahead of 31 May 2021 industry ramp up.
- Review test scenario use cases and look to incorporate within their own testing with e-merchants.
- Complete majority of proposed testing with e-merchants ahead of 31 May 2021.
- Review learnings and observations from TWG testing facilitation (located in appendix 3).

2. Structure of this document

The guidance in this document is structured into three parts:

Appendix 1 - Testing scenario use cases

This section provides e-merchants and issuers with high-level testing scenario use cases which they should consider testing as part of their BAU testing activities.

These will be updated on a periodic basis to include additional scenarios and further refined following any feedback from TWG testing facilitation.

Appendix 2 - 3DS optimal field completion

The UK Finance SCA PMO established a Data Consistency Sub Group, in response to issuers noting increased card holder friction and challenge when enabling their 3DS v2.X flows. The sub group undertook an activity with two large access control server (ACS) providers to ascertain whether there are 3DS fields that are not being completed/completed incorrectly that account for the increased challenge rates.

This appendix provides guidance to e-merchants on 3DS fields completion to reduce card holder challenge rates and improve acceptance rates.

Appendix 3 - Observations and learnings from TWG testing facilitation

The TWG undertook a proof of concept (PoC) to help validate the testing scenario use cases that have been developed and provide some observations and learnings from this to aid those using this document.

As TWG testing facilitation begins to match up issuer and e-merchant participants, the observations and learnings from each partnership will be added to this document to serve as an aid to all.

This appendix will be updated with further observations and learning on a periodic basis and after successful completion of TWG facilitated testing.

3. Appendix 1- Testing Scenario Use Cases (v.2)

Test case	Test Use Case (all including error handling by ACS and 3DSS/Merchant)	Merchant Scope	Merchant	Issuer Authen	Issuer Authori	Test Outcome	UX test cases	Recommended
A.1	Minimum Data	All	Provides required data	Yes	Yes	Checks successful completion with minimum data fields as defined in section 3 and in relevant scheme guides	N/A	Highly
A.2	Exemption flags	All	Uses relevant or supported exemptions	No	Opt.	Checks successful completion of a 3DS exception request (exception used to align with merchant actual exception usage)	N/A	Yes
A.3	Exemption: Low Value Transaction	All	Uses multiple low amount transactions to trigger issuers 1A response	No	Opt.	Checks successful completion of a low value exception request	Opt.	Yes
A.4	Fall-back handling: EMV 3DS version fall-back	All	Merchant needs to have business logic in place to support fall-back	Yes	N/A	Checks successful completion of a secure one-off authentication, when 3DS version 2 is attempted, but not supported by the issuer, and the authentication is then completed using version 1	Yes	Highly
A.5	Fall-back handling: Soft Declines	All	Merchant needs to be have business logic in place to be able to handle soft-declines	No	Opt.	Checks successful completion of a secure one-off authentication, when a straight to authorisation attempt has been declined (soft decline), or an exception has been refused by the issuer	N/A	Yes
A.6	Straight to Auth	All		No	Yes	Checks successful completion of an authorisation sent without 3DS, or authorisations containing an exception request	N/A	Yes
A.7	Basic Guest Checkout	Merchants that offer guest check-out	Initiates basic transaction	Yes	Yes	Checks successful completion of a secure one-off authentication	Yes	Highly
B.1	Card-On-File set up	Merchants that support card-on-file	Storing the card	Yes	Yes	Checks successful completion of a secure authentication where the card is being stored (non-payment authentication)	Opt.	Opt.
B.2	Card-On-File transaction	Merchants that support card-on-file	Using a stored card	Yes	Yes	Checks successful completion of a secure authentication where the card PAN is stored, and the transaction is initiated by the cardholder	Opt.	Yes
B.3	Zero Value Authorisation	Merchants that have non-payment use cases	Other NPA cases	No	Pref.	Checks successful completion of a secure zero value transaction (aka non-payment authentication)	Opt.	Yes
C.1	Subscription - Trial	Merchants that support subscriptions	Merchant initiates subscription trial event	Yes	Yes	MIT Framework - Checks successful completion of a secure authentication where the card is being stored for a trail subscription	N/A	Opt.
C.2	Subscription - Start	Merchants that support subscriptions	Merchant activates paid subscription	Yes	Yes	MIT Framework - Checks successful completion of a secure authentication where the card is being stored for a subscription	N/A	Opt.
C.3	Subscription - Renewal	Merchants that support subscriptions	Merchant initiates a renewal MIT authorization trx	No	Yes	MIT Framework - Checks successful completion of a secure authentication where the card is being stored for a renewal	N/A	Opt.
C.4	Subscription - Renewal with Price Change	Merchants that support subscriptions	Merchant initiates a renewal MIT authorization trx with changed amount	Yes	Yes	MIT Framework - Checks successful completion of a secure authentication where the card is being stored for a renewal where the new amount differs	Opt.	Opt.
D.1	Dynamic Linking: Different Merchant IDs	E.g. Travel merchants and marketplaces	#TBC	No	Pref.	Checks successful completion of a secure one off authentication, and authorisation where the Merchant ID differs	N/A	Yes
D.2	Dynamic Linking: Transaction Amount differs	Travel merchants and marketplaces, other merchants (e.g. groceries)	#TBC	No	Pref.	Checks successful completion of a secure one off authentication, and authorisation where the amount differs	N/A	Yes
E.1	Out-of-scope handling	N/A	No activity	Yes	No	Checks that Issuer has business logic in place and can identify and handle out-of-scope transactions correctly – Needs out of region merchant		

Other considerations

UX testing should cover the following OS Browser combinations (recommended versions, and relative market share Dec18-Dec19 for UK)

Operating System	Chrome	Safari	Firefox	IE/ Edge
Windows	V78.0/v79.0 (all versions 29.3% across platforms)	v13 (4.8%)	v71.0 (4.0% across all versions & platforms)	V11/V18 (3.4% / 4.7% across all versions & platforms)
Mac OS				
iOS	iPhone (0.9%) iPad (0.5%)	iPhone (19.7%)* iPad (6.9%)*		
Android	20.1%*	N/A		

Source: statcounter.com, retrieved 2020-01-29; Values do not add to 100%, as some smaller footprint browsers have been excluded
* Version dependant on underlying OS

Recommendation is to cover the most commonly used browsers as per statcounter.com or similar
Highlighted browser/OS combinations cover 73.4% of internet connections. Data may vary by merchant.

Merchant integrations

- **In-App – HTML**
  - With all relevant options for merchants to select screen size as per EMVCo challengeWindowSize parameter (see EMVCo Spec, pg. 195, see below)

EMV 3-D Secure Protocol and Core Functions Specification v2.2.0
3-D Secure Data Elements
Page 195 / 286

Data Element/Field Name	Description	Source	Length/Format/Values	Device Channel	Message Category	Message Inclusion	Conditional Inclusion
Challenge Window Size Field Name: `challengeWindowSize`	Dimensions of the challenge window that has been displayed to the Cardholder. The ACS shall reply with content that is formatted to appropriately render in this window to provide the best possible user experience. Preconfigured sizes are width x height in pixels of the window displayed in the Cardholder browser window.	3DS Requestor	Length: 2 characters JSON Data Type: String Values accepted: • 01 = 250 x 400 • 02 = 390 x 400 • 03 = 500 x 600 • 04 = 600 x 400 • 05 = Full screen	02-BRW	01-PA 02-NPA	CReq = R	

- **In- App- Native**
  - UX controlled by the merchant, so focus should be on out-of-band authentication, error handling and authorisation

4. Appendix 2 - 3DS optimal field completion

E-merchant support of 3DSecure (3DS)[1] is very important in ensuring readiness for online transactions and avoiding declines after SCA is live in the UK before **14 September 2021**. E-merchants should be ready by **May 2021** when payment service providers (PSPs) will begin randomly checking SCA compliance and declining transactions that are non-compliant.

Before that point, e-merchants must decide which version of 3DS they require to meet their compliance needs: version 1, version 2.1, or version 2.2.

3DS v2.1 or v2.2 is recommended due to its ability to reduce friction at checkout compared to v1. However, its benefit over 3DS v1 is not currently being realised due, primarily, to poor data quality and or consistency for data fields which are new to v 2. This guidance aims to provide clarity and best practice for these data usages.

3DSecure supports card transactions for e-commerce but there are alternative solutions available, such as sending transactions directly to authorisations with the correct flag and payments made through Open Banking and other app-based solutions

What is happening today?

Transactions sent via 3DS v2 are currently experiencing higher step-up/challenge rates than 3DS v1. Inconsistency for some data fields has caused issuers' fraud checks to falsely identify these transactions as fraud.

Investigations, led by UK Finance, have identified **three key data fields** which have caused a significant number of errors with 3DS v2. E-merchants, gateways or content management providers must capture and submit this data correctly to avoid declines**.**

Key Findings[2] – 3DSv2 data consistency

1. **The 3DS method URL**: This helps recognition of the browser and device and is not being used by e-merchants – around 30 per cent of transactions sampled did not have this data.

2. **Three key fields**: as detailed in the below table, are either missing, incomplete or inaccurate – observed in 30-80 per cent of transactions sampled.

3. **Remaining Fields**: Other optional, but useful, data fields can also improve the challenge rates.

1 Please refer to the UK Finance Communication on Strong Customer Authentication for further information

2 Findings and recommended actions have been reviewed with Scheme, Gateway, and Merchant representatives in preparation of this guidance.

ID	Title	Volume**	Action	Comments
1	**3DS Method**	~30%	Call the 3DS method URL when authenticating	•The 3DS method URL enables the ACS to recognise the browser device •This is considered essential •This information also allows for recognition returning customers.
2	**Key Fields**	1. ~30% 2. ~40-70% 3. ~50-80%	Aside from the Mandatory fields, completing all of the below: 1. Browser IP (field 21) 2. Shipping & Billing Post code (fields 11 & 26) 3. Address match indicator (Field 27)	•Field 21: The publicly routable customer browser IP is **essential** to the correct operation of the protocol •Field 11 & 26: The inclusion of the first half of the UK post code as a minimum is **essential,** even better with the full post code •Field 27: It is recommended to use address validation. However, if e-merchants are unable to send the full address, information in field 27 provides anonymous indicator to improve accuracy of risk assessment •In the case of 'electronic shipping', the address is expected to be blank (delivery/timeframe = electronic shipping)
3	**Remaining Fields**	~70-100%	As a general rule the completion of as many fields as possible will always help to reduce challenge rates over time. As it will help with the learning of Merchants trends	•In a SCA environment, the e-merchant provision of more fields **consistently and accurately** may increase effectiveness of the issuer TRA exemption (Issuer's TRA exemption threshold is based on their fraud ratios) •Some relevant fields include: merchantName, MCC, acquirerMechantID,

*Volume of 3DS v2 web browser transactions with missing / inaccurate
**Volume of 3DS messaged with Missing / Inaccurate Data

Analysis was focused on Web Browser transactions as the data from Merchant native App transactions is currently too small to be reliable.

Recommendations

E-merchants

- If you are already using 3DS v2, review how you currently capture the data relevant to 3DS v2 data capture and the submissions to address. You should aim to address these errors as soon as possible.
- If you are yet to adopt 3DS v2, please apply this guidance as you move towards implementation to avoid these issues.

Acquirers/gateways/web service content management/Enterprise Resource Planning (ERP) providers

- We recommend that you incorporate this guidance into e-merchant configuration and testing where applicable.
- It is also recommended that you incorporate this in your communications and guidance to e-merchants to support their implementations.

Testing Considerations

It is important to remember that when SCA is being tested or on go live, the following general rules will apply:

- challenge rates are expected to be higher for all versions of 3DS as all transactions without an SCA exemption, or those out of scope, will need to be authenticated as a default position.
- challenge rates for 3DS v2.2 (or v2.1 with extensions) are expected to be lower than 3DS v2.1 and v1 as it allows the additional option to apply an acquirer exemption: transaction risk analysis.

5. Appendix 3 - Observations and learnings from TWG testing facilitation

TWG testing facilitation – REF001 – Proof of Concept 1 ("PoC 1") (Large multinational e-commerce merchant – Large Tier 2 card issuer) – *updated 23/07/2020 (with v.1 of test scenario use cases)*

General observations/comments from PoC 1 issuer:

1. most of the test are very critical to understand if an authorisation system correctly recognises the flags and that its parameters are working as expected to give soft declines or approve them without SCA
2. after the tests we identified some issues relating to exemption flags which we need to investigate and understand the root cause
3. some tests seem to be repetitive and these are indicated in the test observation comments.
4. most scenarios are easy to recreate by an issuer using guidelines given by the e-merchant. However, some complex scenarios, which we believe are necessary, require change and or maintenance at e-merchant side and hence we are not able to test them
5. some tests can be observed better if the e-merchant and issuers have attended the tests and investigated the issues in real time. In general, it requires co-operation from each party to understand the root causes and solve the issues
6. it is very useful to see the card holders journey from both the e-merchant and issuer perspective for soft declines
7. overall, the test plan from an issuer perspective provided comfort on the appropriate areas to test. The testing highlighted some issues which we worked to identify the root cause of and address.

Approach to testing from POC 1 issuer:

1. the issuer was able to reduce customer impact in turning on 3DS flows, as it produces cards for different countries under different organisation codes. The issuer was able to set up their PSD2 parameters at organisation codes level only for one small organisation (where they see very low number of cards) for testing duration and deactivate them after completion of the tests for the day. This was done several times to accommodate for multiple sessions to create each scenario.
2. the issuer used specific production test cards to run these scenarios used cases.

General observations/comments from POC 1 merchant:

1. no comments provided

Approach to testing from POC 1 merchant:

1. no comments provided

REF001 – Proof of Concept 1 – Learnings and observations (redacted)

To obtain a copy of the testing guidance and approach document with learnings and observations from testing included – please contact scapmo@ukfinance.org.uk