

UK SCA Implementation and Ramp Up Plan

November 2020

UK Industry SCA Implementation Plan



Introduction

In the context of the UK rollout of Strong Customer Authentication (SCA), the Financial Conduct Authority (FCA) announced and agreed to a managed rollout for SCA with UK Finance to give the payments and e-commerce industry extra time to implement SCA with minimum customer impact.

In light of the impact of Covid-19 on key stakeholders, and to minimise the impact on both consumers and e-merchants, the FCA has updated its Strong Customer Authentication page to give an additional six months to implement SCA for e-commerce, to a revised date of 14 September 2021. This can be found [here](#).

The FCA statement clearly expects momentum to be maintained but recognises that additional time may be needed due to the impacts of Covid-19.

The UK Finance SCA Programme team has developed this revised detailed implementation plan and the high-level plan. We urge all stakeholders active in e-commerce to take note of the various deadlines and the introduction of a gradual SCA ramp up which will require all parties to be ready by the end of May 2021.

This plan is structured in 3 key phases and focuses on SCA compliance based on scheme-based payments solutions in order to cover the majority of card-based transactions. Therefore the roll out focuses on 3DSecure (as enables issuer authentication and usage of exemptions) and transactions sent directly to authorisations (as enables flagging of exemptions and out of scope transactions).

However, there are other SCA compliant solutions available in the market, such as those provided by Payment Initiation Services (e.g. through Open Banking), Apple Pay and Google Pay.

Executive Summary



UK SCA Implementation and Ramp Up Plan

Following the FCA confirmation of a revised date for UK SCA enforcement to 14th September 2021, there is a need to ensure all parties continue working on the delivery of all elements required for SCA readiness and compliance. For that reason UK Finance PMO has focused on the delivery of two elements:

- 1. UK Implementation plan** – aiming at ensuring all parties are aware of two key points: readiness of all SCA elements is required by May 2021 and UK issuers will start checking randomly from 1 June 2021 whether e-commerce transactions are SCA compliant (non-compliant transactions will be soft-declined).
- 2. UK SCA Ramp up guidance** – raising awareness about the Issuer led SCA ramp up which starts with the activation of low-risk SCA transactions in February 2021 with all SCA transaction flows being activated by May 2021.

The two elements above are crucial foundations to avoid a cliff edge implementation as they are aimed to drive a call to action for e-merchants, acquirers, gateways, issuers and ultimately customers. However it is acknowledged that at least two other critical elements need to be developed to drive a successful outcome:

- 1. Communication** – aiming at delivering an ongoing message to e-merchants which evolves over time
- 2. Monitoring and controlling** – aiming at understanding market readiness and development toward the target environment

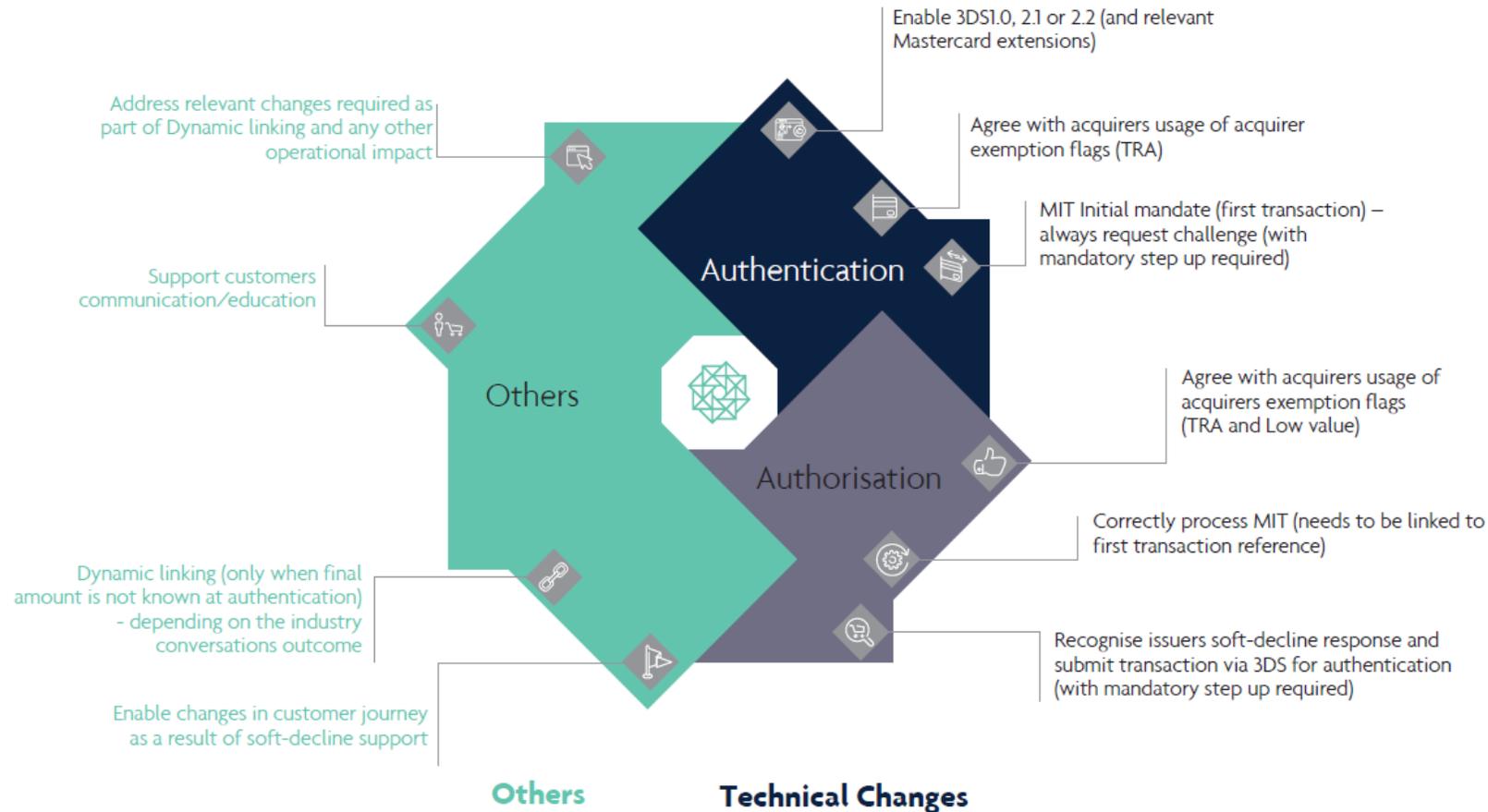
UK Finance's SCA PMO has put in place a programme structure to drive awareness, engagement and the mechanisms to monitor progress

The UK issuer-led SCA Ramp up proposal outlined in this document has been developed to provide the tools to acquirers and schemes to drive e-merchant readiness to avoid a cliff edge implementation by the SCA enforcement date.

The plan focuses on the UK market only. As the SCA enforcement date is 31 December 2020 across the rest of the EU, e-merchants need to check the specific plans in each of the relevant jurisdictions.

UK SCA Readiness: e-Merchants

e-Merchants target position to ensure SCA compliance and support of exemptions



Merchants high level target SCA position is comprised of mandated and optional activities. Merchants should speak with their gateways and acquirers to define and agree their specific SCA readiness requirements.

Implementation Plan

Transaction journeys impacted and approach

Enabling all SCA journeys

Outlining all SCA transaction flows in scope of the SCA Ramp up

Transaction flows			Description	e-Merchant / Acquirer action	Issuer action	Friction	
Authentication (3DS)	SCA exemptions	Issuer exemptions	<ul style="list-style-type: none"> TRA thresholds: <£90, <£215, <£430 Others: trusted beneficiaries, delegated authority 	Via 3DS	TRA Applied	Low	
		Acquirer exemption: TRA ^{LR}	<ul style="list-style-type: none"> TRA (triggered by acquirers – 3DS2.2): <£90, <£215, <£430 		TRA accepted or declined		
	SCA step ups	Above issuer TRA	<ul style="list-style-type: none"> Triggered by issuers 		Transaction stepped up	Medium	
		E-merchant request ^{LR}	<ul style="list-style-type: none"> Triggered by merchants/acquirers and recognised by issuers (e.g. first MIT, soft decline, etc) 				
Authorisation	Correct flagging ^{LR}	Acquirer exemption: TRA	<ul style="list-style-type: none"> All journeys are triggered by e-merchants/acquirers and recognised by issuers TRA threshold based on acquirer fraud ratios LVT exemption up to £30 	Authorisation with correct flag	Transaction to be decided	None	
		Acquirer exemption: LVT					
		Secure Corporate Payment exemption					
		MIT (recurring)					
	Soft declines	CLV	Out of scope	<ul style="list-style-type: none"> Triggered by issuers 	Authorisation with incorrect/no flag	Soft declined (<i>request to send via 3DS</i>) OR Declined (<i>new transaction to be sent via 3DS or correct flag applied</i>)	High
			Total low value exemption (up to £90)				
	Non-flagged	In scope with no exemptions (and issuer unable to authenticate)	<ul style="list-style-type: none"> Issuers will need to soft-decline or decline the transaction 				

UK SCA Implementation Plan Approach

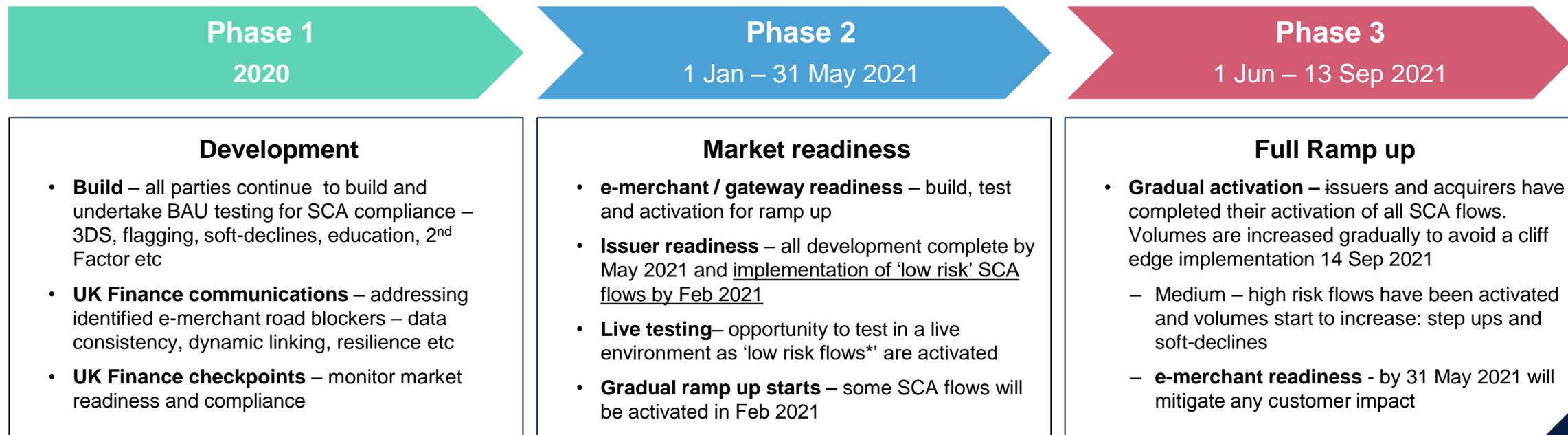
Driving action by raising awareness



Key Objectives

- Ensure issuers understand the key high level milestones and the industry plans for a SCA ramp up
- Ensure issuers continue working towards their SCA readiness by **31 May 2021** (with some elements being delivered in Feb 2021)

Phased Delivery



* Low risk flows: Issuer recognition of acquirer TRA and e-merchant step up request (via 3DS) and correct flagging (via authorisations)

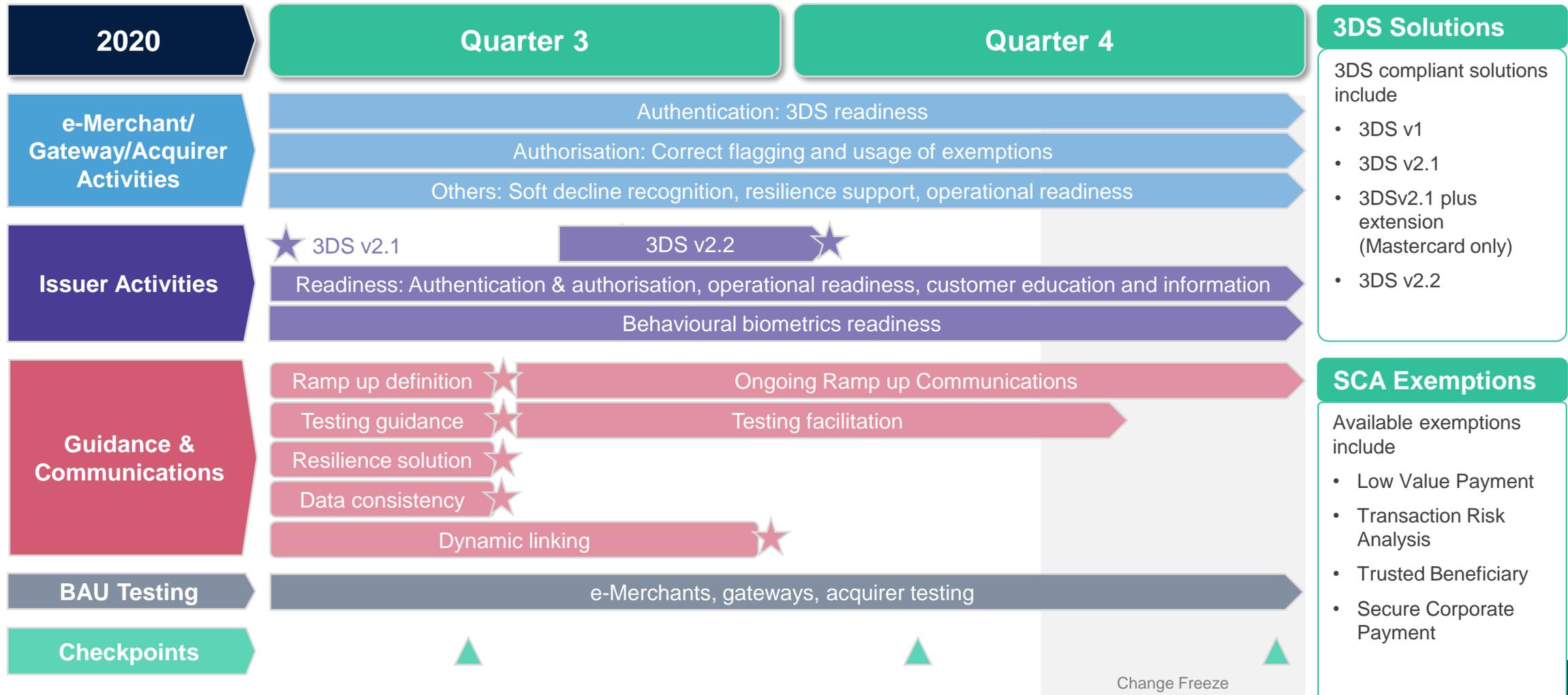
Implementation Plan

Infographic

UK Industry SCA Implementation Plan



UK Only – 2020 activities (The enforcement date is 31 December 2020 across the rest of the EU)

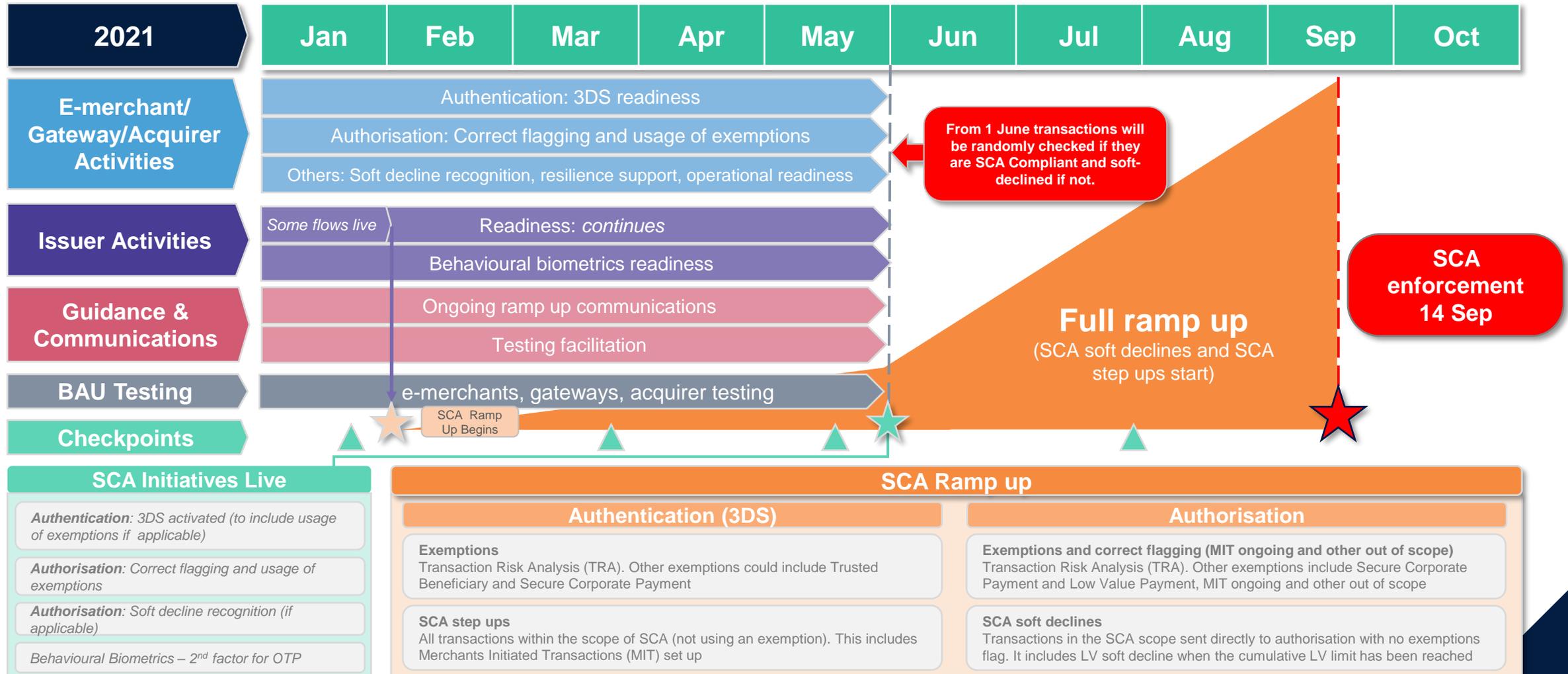


★ Denotes delivery milestone

Through out the period, issuers will continue challenging transactions as per their decisioning strategies

UK Industry SCA Implementation Plan

UK Only – 2021 activities (The enforcement date is 31 December 2020 across the rest of the EU)



Through out the period, issuers will continue challenging transactions as per their decisioning strategies

E-merchant Readiness

3DS and / or correct flagging via authorisations

Strong Customer Authentication

UK readiness overview: 3DS and/or correct flagging via authorisations



- The UK SCA enforcement date is now 14 September 2021, this means **e-commerce transactions that are unable to be authenticated or those without exemptions will be declined after that date.**
- To avoid a cliff-edge implementation by enforcement date, SCA will be introduced gradually (SCA Ramp Up) in the UK from 1 June 2021:
 - UK issuers will start checking randomly if e-commerce transactions are SCA compliant (non-compliant transactions will be soft-declined)
- **e-merchants need to be ready by the end of May 2021** as this will be critical to mitigate any SCA impact, to achieve this merchants need to:
 - Activate 3DS and/or
 - **Correctly flag transactions via authorisations** i.e. acquirer exemptions, out of scope and MIT ongoing

Exemptions	
Exemption	Issuer / acquirer
Low value payment	Acquirer
Transaction risk analysis	Issuer and acquirer
Trusted beneficiary	Issuer
Secure corporate payment	Issuer

SCA Initiatives Required
Authentication: 3DS activated (to include usage of exemptions if applicable)
Authorisation*: Correct flagging (to include usage of acquirer exemptions if applicable)
2nd factor for OTP: Behavioural biometrics (if applicable)

* Acquirers can apply Low Value (LV) and Transactions Risk Analysis (TRA) exemptions for transactions sent directly to authorisations

Strong Customer Authentication

3DS: Enabling authentication and usage of SCA exemptions

3DS

- Enables the issuer to apply SCA
- Facilitates the usage of **issuer** (all versions) and **acquirer** exemptions (version 2.1 plus* extensions and version 2.2 only)
- There are 3 main versions of 3DS in the market:
 - 3DS version 1.0
 - EMV 3DS version 2.1 (and 2.1 with extensions)
 - EMV 3DS version 2.2 (and 2.2 with extensions)
- All 3 versions are SCA compliant, however 3DS v2.1 or v2.2 has features that will reduce friction at checkout compared to version 1



However it is important to remember that SCA compliance can be achieved via enabling 3DS and/or flagging transactions correctly (i.e. acquirer exemptions, out of scope or MIT ongoing) via authorisations

* Mastercard only

Strong Customer Authentication

3DS: Considerations when choosing a version to support



3DS Version	3DS v 1	EMV 3DS v2.1	EMV 3DS v2.2*
Journey optimised for mobile and tablet devices	x	✓	✓
A choice of authentication options can be provided to customers during check out (authentication methods to be defined by issuers)	x	✓	✓
TRA exemption can be applied by issuers	✓	✓	✓
TRA exemption can be applied by acquirers**	x	x	✓
Customer journeys with delayed shipment/delivery (post 90 days) are supported (no need for re-authentication using SCA)	x	✓	✓
MIT set up can be flagged and recognised by issuer. Therefore, customers do not need to be authenticated for MIT series	x	✓	✓
Trusted beneficiary exemption support (if offered by issuer)	x	x	✓
Delegated authentication support	x	x	✓

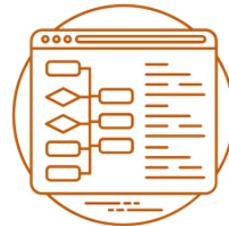
* 3DS v2.1 plus extensions will support most of the functionality of 3DS2.2

** Acquirers can apply TRA exemption directly via authorisations regardless of the 3DS version being used

Second Factor for OTP

Support requested to e-Merchants as part of behavioural biometrics

- Behavioural biometrics is the industry recommended solution as the second factor authentication for (non-app) online transactions when using OTP as an authentication.
- This approach aims to minimise any customer impact during the check out by avoiding the need of customers requiring a static password or their card PIN, in addition to an OTP. Past experience in the UK and internationally has shown this to be highly disruptive, whilst creating new opportunities for fraud.
- Behavioural biometrics solutions will require JavaScript integration for 3D Secure browser-based authentication challenge flows.
- Therefore, e-merchants are encouraged **not to implement restrictions** on their websites that could interfere with such scripts. Possible restrictions could be related to the inclusion of third-party content, CORS restrictions, or similar.



E-merchants are encouraged to ensure that when enabling JavaScripts they do so in a safe manner so as to allow the usage of behavioural biometrics for web browser shopping whilst providing customers with a convenient way of authenticating.

This in turn will avoid the unwelcomed need to use other authentication solutions which could add friction to the customer's online check out experience.



UK SCA Ramp Up: Summary



UK Issuer Led SCA Ramp up Approach

- Issuers to activate low risk SCA transaction flows (recognition of acquirer TRA and e-merchant step up request via 3DS and correct flagging via authorisations) by February 2021
- Issuers to start activating gradually medium (SCA step ups) and high (soft-declines) risk flows by June 2021. This is to give time for e-merchants to be ready with SCA and minimise any impact to customers
- Issuers to enable the 2nd factor for OTP (if applicable) by May 2021

UK Acquirer Role

- Drive e-merchants awareness of SCA implementation and ramp up plan: 3DS and correct flagging by May 2021
 - If e-merchants are ready for SCA, impact of soft declines will be limited

UK Finance Role

- To facilitate and coordinate the delivery of SCA in the UK
 - bringing stakeholders together to enable and support the wider UK market implementation
- Communications: ongoing communication to ensure understanding of SCA Implementation and ramp up plan. Supported via 2 Task Force Groups:
 - Engagement & Readiness Task Force: Gateways and e-merchants
 - Engagement & Readiness Task Force: Issuers and Acquirers
- Monitoring and controlling: to understand readiness and potential impact
 - Industry readiness: define the metrics to monitor issuers and e-merchant readiness towards the implementation plan
 - Ramp up performance: define the metrics to monitor SCA ramp up

Appendix

Data consistency considerations

Data Consistency Background

3DS – Ensuring data consistency to maximise data profiling



Current problems with 3DS2:

- **High Step up/Challenge Rates** – Transactions going through 3DS v2 have had higher challenge rates than 3DS v1. As 3DS transactions are currently challenged based on issuers fraud/risk strategies (Pre SCA), 3DS v1 'should' have similar challenging rates to v2.1 and v2.2.

It is important to highlight that in the SCA environment:

- Challenge rates are expected to be higher for all versions of 3DS as all transactions without an SCA exemption will need to be authenticated
- Challenges rates for 3DS2.2 are expected to be lower than 3DS2.1 and 1 as it allows the usage of acquirers exemptions
- **Data Inconsistency** – There are instances of inconsistent / missing data fields within the 3DS protocol messages across different merchant implementation
- **Benefits of enhance 3DS protocol are not materialising** – e-merchants are reluctant to implement or switch on 3DS v2 due to high challenge rates

Addressing the problem:

A sub-group within the Implementation Task Force was set up with the aim to address e-merchants data consistency as a way to resolve the problems with 3DS. This activity is seem crucial to ensure 3DS2 is leverage appropriately to minimise any SCA impact.

- Identify data consistency issues and how to tackle them
- Define an industry guidance: e-merchants, issuers, acquirers, gateways etc.
- Monitor results/performance based on the guidance provided

SCA Data Consistency

Key findings and remedies for e-merchants to reduce 3DS2 challenge rates*

ID	Title	Volume**	Action	Comments
1	3DS Method	~30%	Call the 3DS method url when authenticating	<ul style="list-style-type: none"> 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	<ol style="list-style-type: none"> ~30% ~40-70% ~50-80% 	Aside from the mandatory fields, completing all of the below: <ol style="list-style-type: none"> Browser IP (field 21) Shipping & Billing Post code (fields 11 & 26) Address match indicator (Field 27) 	<ul style="list-style-type: none"> <u>Field 21</u>: The publicly routable customer browser IP is essential to the correct operation of the protocol <u>Field 11 & 26</u>: The inclusion of the first half of the UK post code as a minimum is essential, even better with the full post code <u>Field 27</u>: It is recommended to use address validation. However if 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	<ul style="list-style-type: none"> In a SCA environment, the 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, acquirerMerchantID,

*Reduction in challenge rates caused by data issues

**Volume of 3DS messaged with Missing / Inaccurate Data

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

Communication approach

Title	Question	Schemes	Acquirers	Gateways
Existing e-merchants	How can they be monitored and improved / remediated	<ul style="list-style-type: none"> • Communication via Acquirer with scheme bulletins and gateway/ e-merchant bulletins • Ad-hoc testing suite available which flagged e-merchants can be invited to 	<ul style="list-style-type: none"> • Updated guidance communicated via: <ul style="list-style-type: none"> • Scheme bulletins to Acquirers • e-merchant comms – point to the implementation guide (website) • Vendor bulletin from acquirer to gateways 	<ul style="list-style-type: none"> • Monitor the field usage and track against approval rates • Updated guidance communicated via <ul style="list-style-type: none"> • Developer websites • e-merchant comms
New e-merchants	How can they be set up in a more robust way / certified more effectively	<ul style="list-style-type: none"> • Update test scripts provided to gateways and e-merchants. 	<ul style="list-style-type: none"> • Update accreditation scripts provided to gateways 	<ul style="list-style-type: none"> • Update accreditation with scripts provided by schemes & acquirers • Engage content management providers and key ERPs