UK Finance communication on requirements for Strong Customer Authentication – Travel & Hospitality – Indirect Bookings Technical Readiness

Date: December 2020

What is Strong Customer Authentication (SCA): A new set of rules that will change how customers confirm their identity when making purchases online.

When does it apply: The rules apply in full for card payments, from 14 September 2021 in the UK and from 31 December 2020 in the rest of the EEA.

Why does it matter to you: If merchants, booking agents and solution providers do not act, non-compliant e-commerce card-based payment transactions will be declined. Implementation of these new rules may require testing and specific changes to your payment process. We therefore encourage you to take ***immediate*** action to ensure you are not at risk of declined transactions which may impact your business.

What should you do: Urgent action should be taken by merchants, booking agents, solution providers and intermediaries with an online presence. Further guidance can be sought from the merchant acquirers, gateways or merchants who undertake indirect sales for travel & hospitality packages.

What does this relate to: This guidance is being provided for travel & hospitality bookings made through an indirect channel (third-party bookings) to help you take the necessary steps to comply with the SCA regulation.

Disclaimer:

This document is not intended to create any binding legal obligations on the part of any stakeholder. In the absence of any industry standard body enabled to provide any guidance/standards on this topic of data passing between booking agents and merchants. The guidance has been prepared by payments industry and travel & hospitality stakeholders in a working group of the SCA Programme Management Office of UK Finance to provide guidance to travel & hospitality merchants, their booking agents and other intermediaries on what upgrades may be needed to enable their systems to continue to make or process payment authorisation requests once the new SCA requirements stipulated by PSD2 become effective for e-commerce transactions from 31 December 2020 within the EEA and 14 September 2021 in the UK.

While the suggested upgrades are intended to satisfy the requirements of participating schemes, card issuers and merchant acquirers (at the time of writing) UK Finance does not accept any liability for any actions taken in reliance upon this document. Merchants and booking agents remain individually responsible for ensuring that their payment processing systems comply with the requirements of all applicable laws and regulations (including PCI DSS, PSD2 and GDPR). Failure to ensure that all necessary and appropriate system upgrades have been made by the effective date could result in payment transactions being declined.

For the avoidance of doubt, the contents of this document do not constitute legal advice, are not intended to be a substitute for legal advice and should not be relied upon as being legal advice.

What is Strong Customer Authentication?

Strong Customer Authentication (SCA) is a new set of rules that will change how customers (personal and business) confirm their identity when making purchases online or consenting to the use of card details held on file to help further protect them from fraud.

Following the implementation of SCA, customers shopping, or banking online will often need to undertake an extra step to confirm their identity. For example, the card issuer or provider (e.g. a bank) may use one of a number of ways to verify a purchase or login, such as a passcode delivered by text message, a phone call to the customer's landline, the use of a card reader or a smartphone app.

Under the new rules all parties are required to make the necessary changes to enable customers to authenticate their transactions in a way that complies with the underlying regulation. Further information on SCA and the managed implementation plan can be found on the UK Finance website.

Call to action: This communication provides important information for travel & hospitality businesses of all sizes, and their suppliers, looking to avoid customer disruption after the UK's Strong Customer Authentication enforcement deadline of 14 September 2021 and the EEA's deadline of 31 December 2020. After this point, card issuers will begin to decline non-compliant transactions. We actively encourage sector participants to read the content of this communication and contact either their payment provider (otherwise known as an acquirer or gateway) or with merchants for whom they supply services. This should be done with urgency due to the implementation lead times and testing period required. Further communications on SCA can be found here.

Who is this communication directed to?

This guidance has been produced **for travel & hospitality merchants** and their solution providers to ensure that all the constituent parts of their eco-system are compliant with PSD2 and to avoid payments originating from indirect sales being declined.

- **Booking agents –** these may include but are not limited to:
    - Online Travel Agents (OTA)
    - Bricks and mortar travel agents with an online presence[1]
    - Travel Management Companies (TMC)
    - Other merchants (e.g., some larger hotel and car rental chains taking bookings on behalf of their franchisees, or an airline facilitating a booking for a hotel or card rental etc.)
    - Other travel & hospitality market players involved in the booking process such as metasearch engines or tour operators if they contribute to the processing of the card transaction.

- **Solution providers** involved in the collection, transfer, processing and/or storage of travel & hospitality bookings and associated payment information on behalf of merchants which include, but are not limited to:
    - Customer Reservation Systems (CRS)
    - Property Management Systems (PMS)
    - Online corporate booking tools

[1] The guidance applies where transactions are initiated through web/app presence. If the transaction is initiated face-to-face, authentication must be done by Chip and PIN (or biometrics in the case of mobile payments).

- Travel content aggregators
- Channel managers
- Global Distribution Systems (GDS)
- NDC[2] aggregators
- IATA BSP
- Software, platform, and payment providers to any of the above solution providers

Background:

From 14 September 2019, changes were introduced to online payments to provide further protection to customers. Under the Payment Service Directive 2 (PSD2), SCA is required where a payment service user (customer) initiates an electronic payment transaction.

However, in the UK, the Financial Conduct Authority (FCA) announced and agreed to provide the payments and e-commerce industry extra time to implement SCA. At the request of the FCA, UK Finance established a Programme Management Office (PMO) to coordinate the UK industry managed roll-out plan agreed in the summer of 2019. The European Banking Authority (EBA) similarly allowed for regulatory flexibility on enforcement until 31 December 2020. The aim was to ensure all parties moved towards full compliance in an orderly manner thus avoiding negative outcomes for both customers and merchants.

The new enforcement date is 14 September 2021 in the UK[3] and 31 December 2020 across the rest of the EEA. As a result, UK card issuers will be required to decline all non-SCA-compliant transactions after 14 September 2021. **All merchants, booking agents, suppliers, acquirers, gateways, and issuing banks or payment service providers must be ready to support SCA** from this date.

This communication outlines what is required, and by when to prepare for the new rules. For more information on the agreed managed rollout in the UK, please click here.

What does SCA require?

Unless the transaction qualifies for an exemption[4] or is out of scope of the regulation, SCA will be required for all online (website or app) card payments[5]. In the travel & hospitality sector this includes:

- Direct sales by the T&H merchant [6]
- T&H bookings through a third party (indirect sale)

Card not present transactions without authentication data or without an applicable exemption **will be declined after 14 September 2021 for the UK** and 1 January 2021 for the rest of the EEA.

[2] NDC (New Distribution Capability), is a travel industry supported program for the development and market adoption of a new, XML-based data transmission standard (NDC Standard) that enables the travel industry to transform the way air products are retailed.

[3] EBA opinion issued in October 2019 provided for enforcement of the new rules to start after 31 December 2020. Most member states are working towards this deadline. Enforcement of the new rules in the UK will commence from 14 September 2021.

[4] Please refer to the Regulatory Technical Standards on strong customer authentication and common and secure open standards of communication or UK Finance's upcoming guidance for more information about SCA exceptions and exemptions

[5] Card payments also include payments done with card credential already on file at a merchant.

[6] In this document the word "merchant" is used to designate the Travel & hospitality supplier when it processes the transaction as a "merchant". Note that when the booking agent collects funds as a "merchant of record" in an authorisation on a travel booking, the booking agent becomes a merchant as well.

What does this mean for Travel & Hospitality merchants and their indirect channel sales?

- Merchants must upgrade to solutions enabling them to send payment authorisation requests with the appropriate authentication data.
- Merchants will no longer be able to send payment transactions that originated as ecom/mcom card not present bookings either as "MOTO" (Mail Order & Telephone Order) or simple CNP (Card Not Present) transactions without authentication data (e.g. airline sales) or through manual PAN key entry using their point of sale solutions (e.g. hotels, car rental or other supplementary sales on a travel booking).
- Where bookings and purchases are made through an online or mobile booking channel, authentication is generally performed using 3DS[7]. For face-to-face payments, such as those performed at a physical travel agent, authentication must be performed using two factor authentication such as Chip and PIN[8].
- For Merchant Initiated Transactions (MITs), the payment is initiated by the payee based on pre-existing authority and the payer is not involved in the initiation of these transactions. As with Direct Debits, if the authority for the payments is provided electronically (such as with online subscription services), then the action of granting the authority will be caught by SCA requirements. This means that an authentication challenge (also called a "stepped up" authentication") must take place when the cardholder agrees to pay any fees associated with the booking for the merchant to process with those transactions.
- Upfront deposits, balance payments and cancellation fees processed[9] by T&H merchants[10] may qualify as an MIT.
- Unless the transaction can otherwise qualify for any other exemption or is out of scope.[11], authentication will be required and the authentication data and/or reference to it must be present in each MIT.

Performing Authentication

There may be other compliant solutions available. However, to help guide the sector three possible solutions are provided below:

1. The "booking agent" may send booking details directly to an e- merchant. In order to perform the transaction in a compliant manner, the merchant may send a website or portal link to a customer in order to perform authentication. This would remove the requirement to upgrade to an integrated payment solution.

[7] Further information on 3D Secure can be found here. It is recommended that EMV 3DS 2.2 is supported to ensure both the best cardholder interface experience and that all Travel & Hospitality use cases can be supported for all payment brands.

[8] In the case of mobile payments, biometrics through smartphones may be used.

[9] This also applies to full payment at end of stay/ rental (and delayed charges) if check-in is performed without cardholder present/authentication.

[10] Or GDS, for airline ticket sales.

[11] The transaction can be considered out of scope if 1) done with an anonymous card (e.g. prepaid card); 2) if the booking is done through mail or telephone order; 3) if either (or both) the issuer of the card or the merchant's acquirer is located outside of the EEA or the UK. An exemption may apply if the transaction originated from a secure corporate process or protocol (e.g. from a qualifying Travel Management Company or Online booking Tool). If the merchant or booking agent is to process any MITs, no other exemption can be used.

2. The booking agent may perform authentication with the cardholder and collect *all* required payments on behalf of the travel supplier, e.g at booking, at a pre-agreed date or an agreed time in the event of a cancellation or ‘no show’ charge being applied.

3. The booking agent may perform SCA and pass authentication data and other transactional data, to the merchant to enable the merchant[12] to request/perform an MIT to collect payment as agreed with the customer
    - This may include the booking agent collecting some funds at the point of booking however, authentication-related data must be passed to the merchant as the data will be required to process future payments (MITs, e.g. balance payment or full payment associated to a check-in performed without face to face interaction).

Failure by merchants or booking agents (in the event the booking agent collects payment as a merchant of record) to present authentication data in their payment transactions (or a reference to it) could result in their payment transactions being declined.

Merchants and booking agents should discuss how best to upgrade their payment processes and solutions to meet SCA compliance with their payment service provider and other solution providers. There may be other compliant solutions, however, this document provides guidance on data that must be passed between booking agents and merchants to meet compliance, where **the third option above** is the chosen solution.

The appendix provides further information including the relevant data fields that you will need to be familiar with to comply

[12] Or GDS, for airline ticket sales.

Appendix

The information contained in the appendix further supplements the detail provided in the main guidance where the merchant requests that the booking agent performs authentication on their behalf, but will process payments themselves. Unless otherwise stated, the content provided is in the context of Travel & Hospitality.

How is operational readiness achieved - transactions originating from indirect bookings?

Authentication Requirement

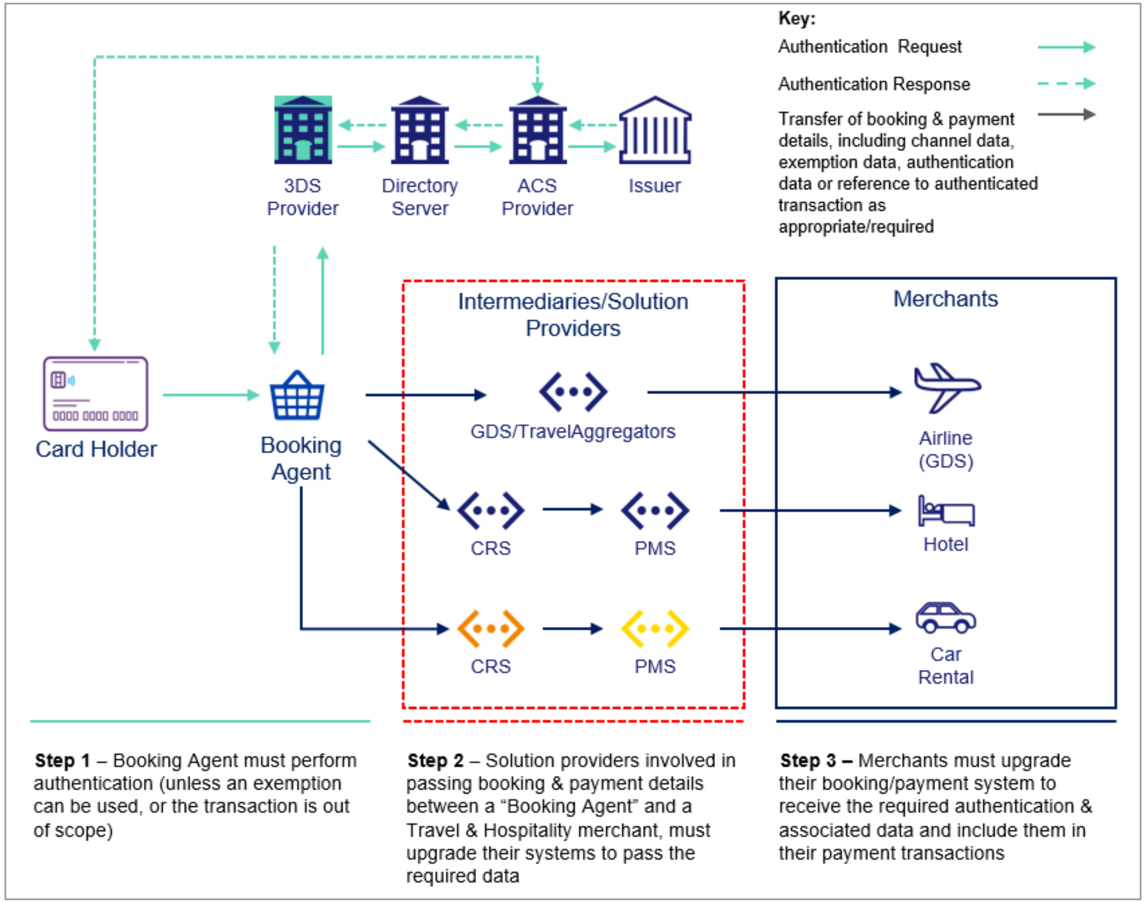
Booking agents need to be able to request authentication through 3DS for all in-scope transactions by the enforcement dates13. Booking agents and merchants should agree upon the role they will play in the authentication and authorisation process with their authentication provider and acquirer and raise awareness of the impact on in-scope transactions. It is recommended that EMV 3DS 2.2 is supported to ensure both the best cardholder interface and that all Travel & Hospitality use cases can be supported for all payment brands.

The next step in meeting readiness requirements is ensuring a mechanism is in place that enables authentication data to be sent and/or received between booking agents and merchants. This may involve intermediaries and merchants upgrading their systems to enable the passing of such data in order to receive and submit payment authorisations with the appropriate authentication data as well as other associated data e.g booking information.

When the authentication of a remote indirect booking transaction is completed by a booking agent, an authentication code, Electronic Commerce Indicator (ECI) value and other associated information are returned by the authentication provider to the booking agent. This “authentication data” needs to be sent to the merchant, along with information relating to the context of the transaction to enable submission in a subsequent payment authorisation request(s) to prove that authentication has been performed. In cases where the booking agent processed the payment authorisation, it may still be necessary to send details of the authenticated payment to the merchant in the event that further associated payments are processed by the merchant at a later time or date.

There may be different data requirements depending on the characteristics of the transaction as defined below. This means all intermediaries and **solution providers involved in passing booking and payment details between the booking agent and the merchant** must upgrade their systems to pass the required data as illustrated in Figure 1:

[13] Unless all the travel & hospitality merchants for which they provide booking services for select option 1 above as a way to process (SCA compliant transactions)



Step 1 – Booking Agent must perform authentication (unless an exemption can be used, or the transaction is out of scope)

Step 2 – Solution providers involved in passing booking & payment details between a "Booking Agent" and a Travel & Hospitality merchant, must upgrade their systems to pass the required data

Step 3 – Merchants must upgrade their booking/payment system to receive the required authentication & associated data and include them in their payment transactions

What system and process upgrades are required to pass authentication and associated data from the booking agent to the merchant?

This section describes the actions that booking agents, solution providers and intermediaries passing data between each other need to take to ensure merchants can process payment authorisation requests in a compliant manner.

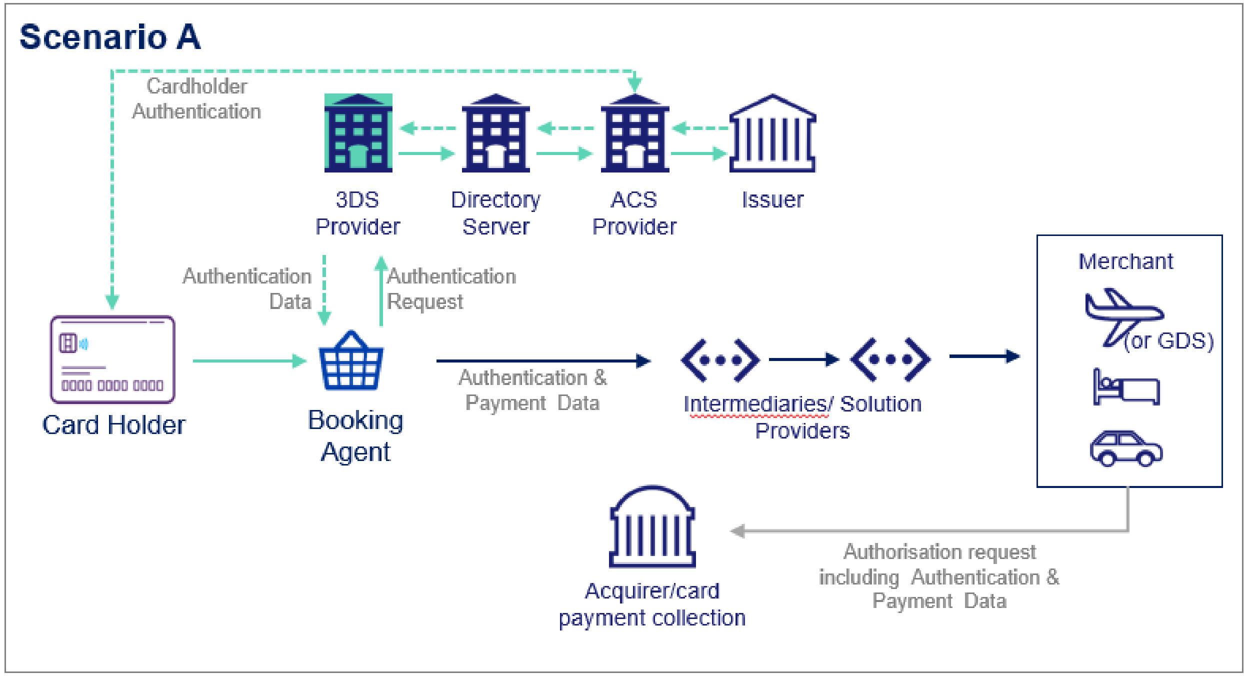
Requirements on booking agents

In order to support authentication, booking agents should work with an EMV 3DS Authentication Provider to define what data is required for each authentication request. The payment and authentication data that needs to be passed to the merchant, directly or through intermediaries, will vary depending on which of the following three scenarios apply:

Scenario A[14]: The booking agent authenticates the cardholder, and the supplier of the travel & hospitality service collects the payment as the "merchant of record".

[14] This scenario also applies if the secure corporate exemption is used through 3DS prior to authorisation.

In this scenario the booking agent must send the relevant authentication data to the merchant either directly or through intermediaries to enable the merchant15 to either request payment authorisation and collect the funds associated with the booking or to set up the authenticated MIT agreement for a later authorisation16

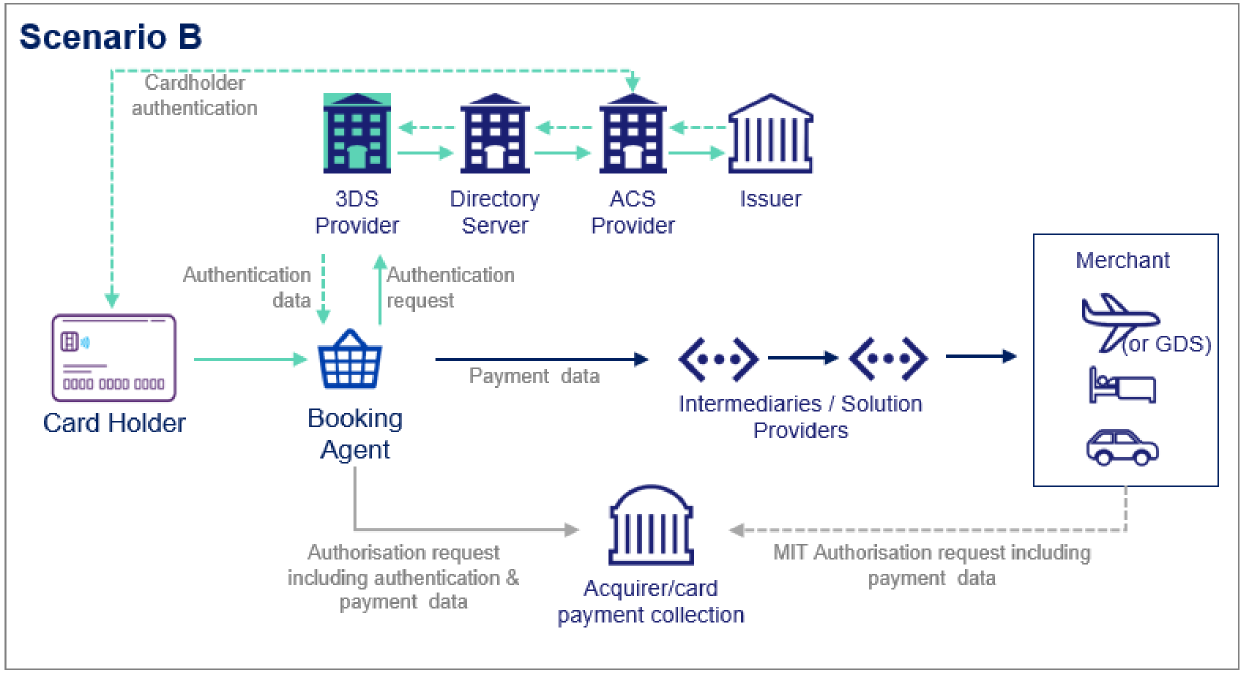

Scenario A
Cardholder Authentication
3DS Provider
Directory Server
ACS Provider
Issuer
Authentication Data
Authentication Request
Card Holder
Booking Agent
Authentication & Payment Data
Intermediaries/ Solution Providers
Merchant
(or GDS)
Acquirer/card payment collection
Authorisation request including Authentication & Payment Data

Scenario B: The booking agent authenticates the cardholder and processes an authorisation to either collect a payment (full or partial) from the customer on behalf of the T&H supplier. This also applies to the setup of an MIT agreement for a merchant to collects funds at a later time.

[15] Or GDS, for airline ticket sales.

[16] If funds are not due at booking, the merchant is still asked to process a transaction to indicate that an MIT agreement has been put in place. This is done by processing a zero value/account verification transaction.

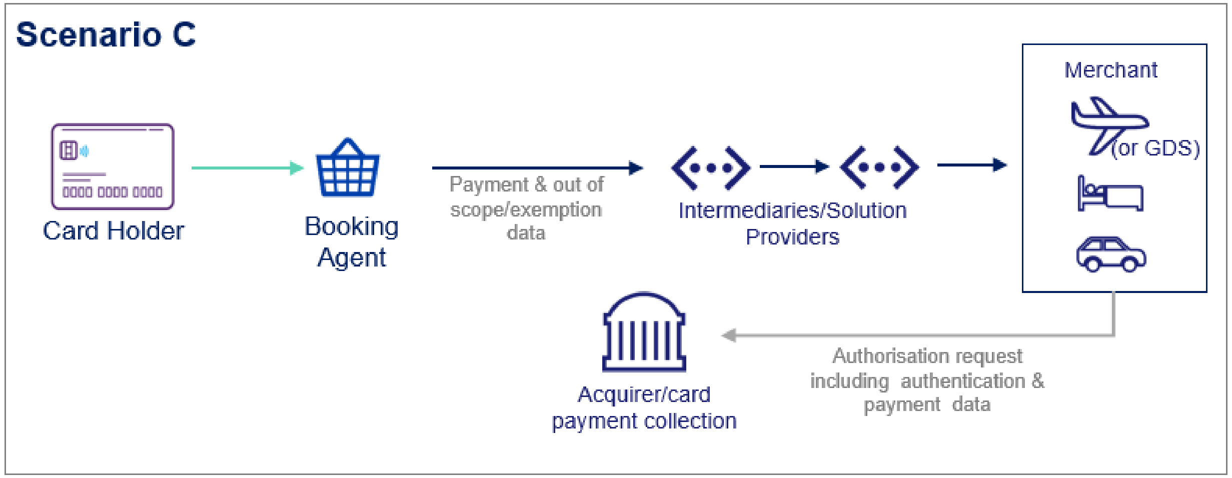
Following authentication, the booking agent requests payment authorisation to collect funds associated to a booking and/or to informs the respective card issuer of the setup of an MIT agreement17. As a next step, the booking agent passes the associated authentication and payment data to the merchant to enable them to collect any additional payments it is authorised to collect, as an MIT, under the terms of the booking agreement with the customer.


Scenario B
Cardholder authentication
3DS Provider
Directory Server
ACS Provider
Issuer
Authentication data
Authentication request
Merchant
(or GDS)
Card Holder
Booking Agent
Payment data
Intermediaries / Solution Providers
Authorisation request including authentication & payment data
Acquirer/card payment collection
MIT Authorisation request including payment data

Scenario C: No authentication is performed by the booking agent as the transaction is out of scope (MOTO, or anonymous transaction) or qualifies for an exemption (e.g. secure corporate payment) and the supplier of the travel & hospitality service collects the payment.

[17] Where no funds are due at the time of the booking, the merchant is still required to process an authorisation transaction to indicate to an issuer that an MIT agreement has been put in place (this agreement must be authenticated). This is achieved by processing a zero value/account verification authorisation transaction which carries authentication data and returns a unique transaction identifier.

In this scenario, the data relative to the out of scope/exemption must be passed onwards to the T&H merchant18 along with other payment data for the T&H supplier to perform their own authorisation request as the merchant of record.19


Scenario C
0000 0000 0000
Card Holder
Booking Agent
Payment & out of scope/exemption data
Intermediaries/Solution Providers
Merchant
(or GDS)
Acquirer/card payment collection
Authorisation request including authentication & payment data

Note: booking agents are not to request exemptions at the authentication stage of a transaction where they are not responsible for the collection of funds, unless they have a specific agreement with the T&H supplier (the merchant). The use of exemptions will be determined by the merchant acquirer in conjunction with their merchant. The secure corporate payment exemption may be applicable if the booking is initiated through a secure and dedicated corporate process or protocol made available to payers who are not consumers. Typically, only transactions associated with bookings that originated from Travel Management Companies (TMC's) and Online Booking Tools (OBTs) may qualify for the exemption.

[18] Or GDS, for airline ticket sales.

[19] This scenario also covers instances where there is an authentication outage in the acceptance flow and authentication could not be performed.

Each of the scenarios outlined have their own data requirements. The respective data must be provided to merchants either directly or indirectly, through intermediaries as defined in **Table 1.** At time of writing[20], booking agents must ensure:

- All data elements marked as "R" (Required) for a payment scenario must be obtained and passed for this scenario
- Data elements marked as "C" (Conditional) for a scenario must be sent when the specific condition applies as noted in Table 1
- Data elements marked as "RM" (Recommended) are recommended to be sent if they are available:
    - As per current business practice of the booking agent or
    - As per the booking agent's agreement with the merchant on whose behalf they process the booking.

Requirements on Solution providers involved in passing booking and payment details from "booking agents" to merchants

Solution providers will need to be ready to *receive any* of the data elements detailed in Table 1 from booking agents and to *pass all data* received to merchants or their intermediaries. Not every data field will be populated in every booking scenario (further detail provided in the table). The data requirements should be discussed with the travel merchants for whom booking agents perform services for, to ensure all requirements meet the merchant's PSPs guidance.

When are the upgrades required?

Merchants should receive the required authentication and associated data and include the fields in their payment authorisation requests by the enforcement dates. Failure to do so could result in payments being declined.

For the enforcement dates to be met, it is essential the upgrades required to receive and pass the data from booking agents to merchants is completed as soon as possible. Solution providers should work with the other upstream and downstream providers with whom they exchange payment transaction data to agree the earliest possible integration timelines.

It is acknowledged that some booking and payment processing workflows involve multiple intermediaries and platforms operating between the booking agent and the merchant. It is also understood that some intermediaries and platform providers may be unable to complete the updates necessary to enable merchants to receive the required data by the enforcement dates. **Interim solutions will be made available** by the payment's schemes to ensure that transactions are not declined due to lack of authentication data/or reference to it where this cannot yet be provided. Solution providers should take note however that these solutions will be applied **for a limited period only and that over time payment schemes may apply measures to acquirers/merchants that encourage the necessary upgrades**. As merchants will not be able to rely on those interim solutions in the long term, solution providers are strongly encouraged to apply updates as early as possible to ensure that they offer their merchant customers compliant solutions.

[20] Booking agents should always discuss with their merchants/ PSPs to ensure they can pass the data required by Schemes at any point in time. Should more data be required, the data table below recommends fields are reserved for future use so that any new required data can easily be added.

Our next steps:

UK Finance will continue to work with the industry to track progress against the agreed delivery plan. Further detailed guidance, including the timelines for interim milestones as well as coordinated testing and live-proving support will be shared in due course.

For further details on the EBA opinions and other UK Finance Programme Management Office (PMO) updates, please visit our website here:

https://www.ukfinance.org.uk/strong-customer-authentication

Data Table 1

Table 1 – Data elements that must be passed from booking agents to merchants (directly or by intermediaries)

Table 1 below outlines guidelines on the specific authentication and associated payment data that solution providers and intermediaries should receive and pass on to merchants, following an indirect booking. This is based on required data for processing PSD2 SCA compliant transactions with major card brands (American Express, MasterCard and Visa), as at time of publication. Please check with each brand (including others who may not have participated in producing this document) on latest requirements and reserve fields for future use to easily accommodate any new data requirements.

The key is for each of the data elements described in this table is passed between booking agents and merchants. Entities are allowed to do this in their own way, using their own specification/codes if they have such artefacts.

In the absence of any other specification, this document is provided as an indication of all the information that must be catered for, enabling a common understanding and usage between multiple parties.

⚠

> While each data element will not be present in each booking, providers must be able to receive and send all the data elements detailed in this section. In order to avoid future upgrades, it is recommended that fields are reserved for “future use”.

Note that all applicable laws, rules, regulations, directives, and governmental requirements relating in any way to the privacy, confidentiality, security, and protection processing of personal data must be adhered to. In particular, service providers must develop cardholder data sharing, processing and storage methods, systems, and infrastructure with respect of the Payment Card Industry Data Security Standards (PCIDSS and PCI3DS).

It is recommended that recipients of these data elements put in place logic to detect erroneous or missing data and set up processes to report such incidents back to the sender. The data, whether erroneous or missing, needs to be passed on to the merchant to determine appropriate actions that need to be taken:

- Whether a transaction can proceed to payment without authentication, with the risk of non-compliance and/or declined
- Or, if a consumer needs to be contacted and authenticated

Data	Field Name	Type and Length	Required (R) Conditional (C) Recommended (RM)	Payment Scenarios	Additional Information
1	Card number or Token Number	30 numeric	R	A, B, C	Either a card number or a token number is provided, not both. (A token number is formatted exactly as a card number)
2	Card Brand	25 alphanumeric	RM	A, C	If info available on card brand selected by the cardholder, the name of the card brand should be passed to respect the regulated customer selection and transaction switching. A maximum of 25 alpha numeric characters are used to convey the message to the party receiving it. This is guidance only to ensure that name of card brand can be passed when known, but you may use other agreed industry format to convey this information if available/ appropriate.
3	Card expiry	4 numeric (YYMM)	R	A, B, C	
4	CVV2/CVC2 value	Max 4 numeric	RM	A, C	SCA is not changing the requirements for CVV2/CVC2. Merchants should continue to provide CVV2/CVC2 where they used to provide it. This data element is indicated as recommended only (not required). Booking agent to discuss requirements with merchant who should in turn discuss with their acquirer

Data	Field Name	Type and Length	Required (R) Conditional (C) Recommended (RM)	Payment Scenarios	Additional Information
5	Channel - *One of the following values is required*	2 alphanumeric - predetermined values as follows:	R	A, B, C	This field indicates in which channel the booking was performed. Only one value must be used.
5.1	Mail order (paper mail, fax and email) or	"MO"			
5.2	Telephone order/IVR or	"TO"			
5.3	Ecom or	"EC"			
5.4	Face-to-face	"FA"			
5.5	Be ready to accept new value that could be created over time	2 alphanumeric			
6	Card or Token number collection method. *One of the following values are required*	1 alphanumeric – predetermined values as follows:	R	A, B, C	This field determines how the card or token number was collected for the transaction.
6.1	Keyed in for this transaction	"K"			
6.2	Card on file (previously stored credentials)	"S"			Merchant receiving card on file should check with its acquirer if it is considered card on file for each scheme as it may not apply to all.
7	Exemption Indicate if any exemption was used. *One of the following value must be used if an exemption is used or if delegated authentication is used*	2 alphanumeric – predetermined values as follows:	C - must be present if an exemption was used	A, C	This field determines which PSD2 SCA exemption was used (EU Only) Before using any exemption or Delegated authentication, a booking agent must ensure the acquirer of the merchant is allowing use of this exemption. It is plausible that in many cases, no exemption is used.

Data	Field Name	Type and Length	Required (R) Conditional (C) Recommended (RM)	Payment Scenarios	Additional Information
7.1	Transaction Risk Analysis Exemption	"TR"			These exemptions cannot be used if subsequent MITs need to be performed by the merchant. Can only be used if the merchants need to authorize a payment immediately with the authentication data and will not need to do any MITs.
7.2	Trusted Beneficiary Exemption	"TB"			
7.3	Low Value Exemption	"LV"			
7.4	Secure Corporate Exemption	"SC"			This exemption can only be used if the Booking originated from Secure Tools and Processes
7.5	Delegated authentication	"DA"			
7.6	Be ready to accept new value that could be created over time	2 alphanumeric			
8	Customer Mandate Indicate if/what kind of mandate was entered into. *One or several of the below values is required (i.e. more than one value can be used if more than one purpose to the agreement. However, if 8.1 is used, only one value must be used)*	2 alphanumeric (more than one value could be possible, comma separated) - predetermined values as follows:	R	A, B, C	This field describes the agreed mandate (if any) between the cardholder and the agent/third party. If there is no mandate, data element 8.1 conveys there is no mandate.
8.1	No agreement/ mandate for future MIT	"NA"			
8.2	Agreement / mandate for future No Show/ Cancellation Fee	"NS"			

Data	Field Name	Type and Length	Required (R) Conditional (C) Recommended (RM)	Payment Scenarios	Additional Information
8.3	Agreement/ mandate for any payments due after check-in to cover charges during stay	“AC”			Where a merchant wishes to facilitate a check-in without customer having to come present his card face –to –face (and authenticate) the cardholder must have agreed at booking time that the card could be used to cover any charge associated with the stay/rental. If no such agreement is in place, the cardholder must present card at check-in and be authenticated.
8.4	Agreement/ mandate for any payments due after check- out (i.e. delayed charges)	“CO”			Where a merchant wishes to facilitate a check-in without customer having to come present his card face –to –face (and authenticate) the cardholder must have agreed at booking time that the card can be used to cover any charge after checkout (delayed charges). If no such agreement is in place, either delayed charges cannot be charged, or the cardholder must present their card at check-in and be authenticated to enable payment of potential delayed charges
8.5	Agreement/ mandate for prepayment/balance payment	"BP"			
8.6	Agreement for recurring payment (fixed date and fixed amount)	"FR"			
8.7	Agreement/ mandate for recurring payment (fixed date and variable amount)	“VR”			
8.8	Agreement/mandate for recurring payment (usage based/ non fixed date and variable or fixed amount)	"UR"			

Data	Field Name	Type and Length	Required (R) Conditional (C) Recommended (RM)	Payment Scenarios	Additional Information
8.9	Be ready to accept new value that could be created over time	2 alphanumeric			
9	Identifier of authorisation (Authorisation Trace ID/Authorisation Trans ID)	16 alphanumeric and special characters, values returned from initial authorisation response	R	B	This field describes the Transaction ID/Trace ID of the authorisation request when performed by the booking agent. This is not the Directory Server Transaction ID. The Tran ID/Trace ID is only present if an authorisation response message (scenario B only). There is no restriction on the duration validity of this data element.
10	Merchant Name used by authenticator in authentication request	40 alphanumeric characters	C – to be present if requested by the scheme	A, B, C	
11	3DS Authentication value (e.g. Cryptogram MasterCard: AAV; American Express: AEVV; Visa: CAVV)	28 characters. A 20-byte value that has been Base64 encoded, giving a 28-byte result American Express AEVV – 20-byte unsigned binary	C - must be present for all transactions indicated as EC on data element 5.3 May optionally be present in other cases (e.g. if Authentication is performed by decoupled authentication for MOTO)	A	The type and length are as per EMV 3DS specification. This should be sent as is to the entity that will process the payment. This entity generally needs to convert this into the authorization format required for each scheme. Note that in the Visa system, if the transaction is done with a Visa Network Token, a TAVV (data element 12) may be present instead of a CAVV or in addition to a CAVV.
12	Authentication Value for Tokens (e.g. TAVV)	28 characters. A 20-byte value that has	C - to be present if required by the	A	Required only for Visa at this time.

Data	Field Name	Type and Length	Required (R) Conditional (C) Recommended (RM)	Payment Scenarios	Additional Information
		been Base64 encoded, giving a 28-byte result	scheme for token transactions AND if transactions indicated as EC in data element 5.3		Within the Visa system, when a transaction is performed with a token, the authentication value may be a TAVV instead of a CAVV therefore, a separate data element is planned for to enable passing of this data. In some instances, a transaction done with a token could have gone to 3DS and have both a CAVV and a TAVV. Booking agents will need to pass on the data they receive.
13	ECI Value	2 numeric characters - Possible values (00 to 09)	C - must be present for all transactions indicated as EC on data element 5.3	A	Value should be populated as received in authentication response. Values may be different by payment scheme.
14	3DS transaction ID Value returned by the 3DS Directory Server	3DS V1 will provide XID value (XID not required for MasterCard) 3DS V2 will provide DS Transaction ID Amex: 20 Bytes unsigned binary MasterCard: 36 characters from EMV 3DS are carried as such into an ISO8583 ans-36 field	C - to be present if 3DS authentication was carried out and if required by scheme in transaction data	A, B	
15	3DS Program Protocol version	3 alphanumeric (no dots in between values)	C - to be present if required by the scheme	A	This may be required in authorisation request for certain schemes.

Data	Field Name	Type and Length	Required (R) Conditional (C) Recommended (RM)	Payment Scenarios	Additional Information
16	Cardholder Billing Address	Further field split provided below	Required in AVS Market (US and Canada) - Recommended in other markets unless market or regional mandate restricts sending this information	A, B, C	It is important to note that when sent for markets where it is not required, it must be correct else better to leave empty.
16.1	City	Variable, maximum 50 characters			
16.2	Country	3 characters (Shall be the ISO 3166-1 numeric three-digit country code)			
16.3	Email	Variable, maximum 254 characters			
16.4	FirstName	2–45 characters			
16.5	Last Name	2–45 characters			
16.6	Post Code	Variable, maximum 16 characters			
16.7	State (if Applicable)	Variable, maximum 3 characters. Should be the country subdivision code defined in ISO 3166-2. Not required, if state			

Data	Field Name	Type and Length	Required (R) Conditional (C) Recommended (RM)	Payment Scenarios	Additional Information
		not applicable for the country			
16.8	Street1	Max 50 characters			
16.9	Street2	Max 50 characters			
16.10	Street3	Max 50 characters			
17	Authentication Issues	2 alphanumeric character – predetermined as follows	C – when there is an authentication outage as defined in additional information for each defined element	C	
17.1	Authentication Outage	”AO”			Use to indicate when authentication was attempted but there was an outage in the authentication flow between the merchant-gateway-3DS Server-DS connectivity flow (or directory server itself), which meant authentication could not be performed or an authentication response could not be received. This is not a formal exemption but information for issuers to consider.
17.2	Be ready to accept new value that could be created over time to convey other	2 alphanumeric			

Data	Field Name	Type and Length	Required (R) Conditional (C) Recommended (RM)	Payment Scenarios	Additional Information
	authentication issues as they may be created from time to time				
18	Purchase/ Transaction Amount	12 numeric characters	R	A, B, C	
19	Purchase/ Transaction Currency	3 numeric characters, ISO 4217 three-digit currency code, other than those listed in Table A.5 of EMVCO 3DS Guide.	R	A, B, C	
20	User Defined Field 1	25 alphanumeric	R		Reserved for future use
21	User Defined Field 2	25 alphanumeric	R		Reserved for future use
22	User Defined Field 3	25 alphanumeric	R		Reserved for future use
23	User Defined Field 4	25 alphanumeric	R		Reserved for future use
24	User Defined Field 5	25 alphanumeric	R		Reserved for future use