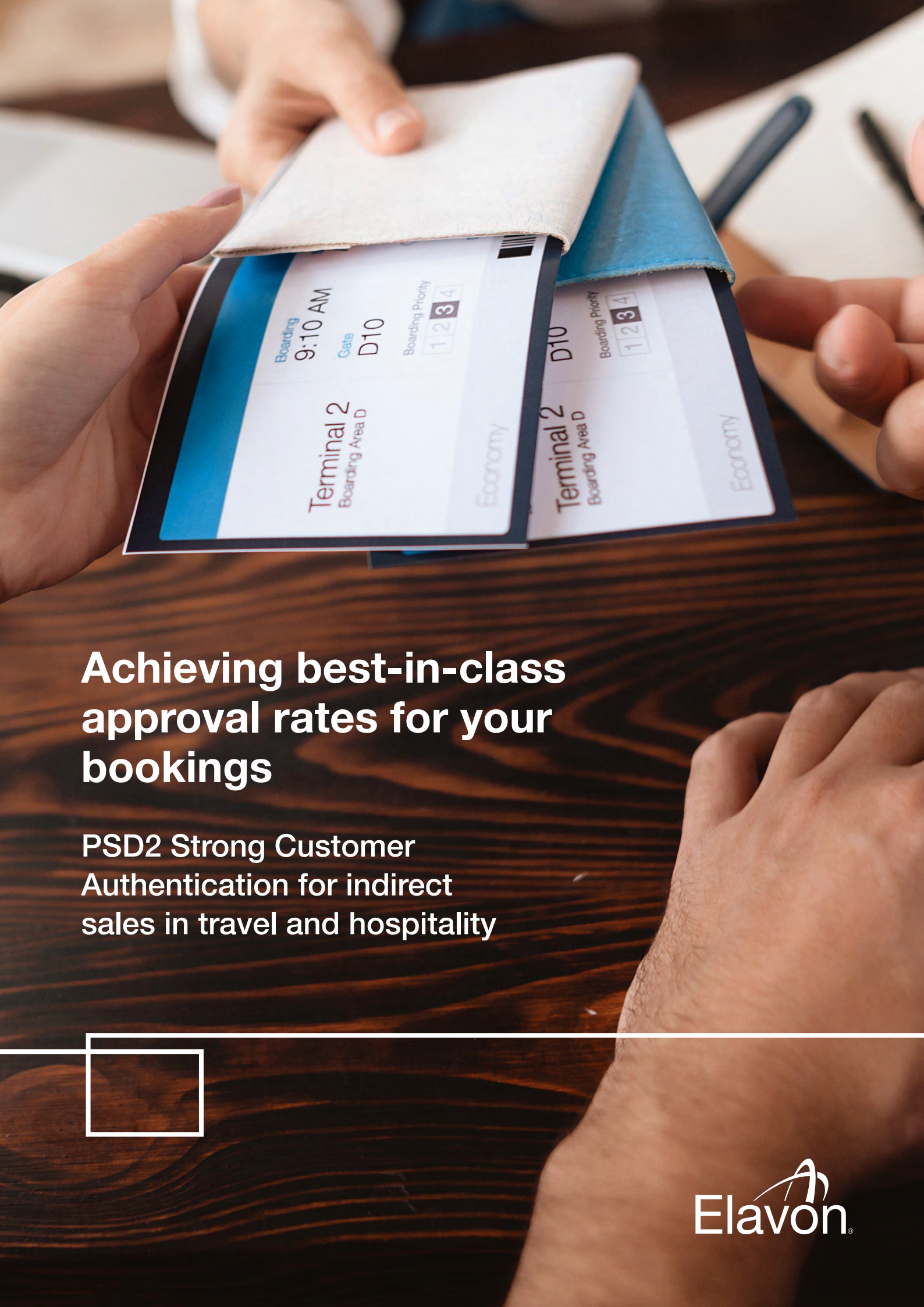


Achieving best-in-class approval rates for your bookings

PSD2 Strong Customer Authentication for indirect sales in travel and hospitality

Elavon®

Contents

04 About this guidance: who needs to take action?

05 Getting ready for PSD2 SCA compliance

07 PSD2 SCA scope, impacts and implications

09 The T&H journey towards SCA compliance: the story so far

10 Your booking agent authentication options reviewed

11 Technical guidance for Option 3

14 Updates required from booking agents, merchants and their solution providers

18 Data requirements

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

21 Data table 1

Notice of Disclaimer

As a new regulatory framework in an evolving eco-system, the requirements for SCA still need to be refined for some use-cases.

This document and any statements represents Elavon's evolved thinking, but it should not be taken as a definitive position or considered as legal advice, and it is subject to change in light of European regulator and the National Competent Authorities guidance, opinions and clarifications. 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, this guidance has been prepared by payments industry and travel & hospitality stakeholders in a working group of the SCA Programme Management Office of UK Finance. It is intended to provide guidance to travel and 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 following the enforcement of the SCA requirements stipulated by PSD2 for e-commerce transactions from 31 December 2020 within the EEA and 14 March 2022 in the UK. Although prepared by a UK based working group, the guidance is valid across the world for any stakeholders engaged in bookings that involve UK/EEA issued card and acquired transactions.

The data elements and guidance within this document were published by UK Finance UK Finance communications on requirements for Strong Customer Authentication - Travel & Hospitality – indirect Bookings Technical Readiness December 2020. The guidance has been supplemented with further information provided by Visa Implementing Strong Customer Authentication (SCA) for Travel & Hospitality June 2021. Note that these data requirements are common across the major card schemes (Visa, MasterCard and American Express).

While the suggested upgrades are intended to satisfy the requirements of participating schemes, Issuers and Acquirers, Elavon 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. Any case studies, statistics, research and recommendations are provided 'AS IS' and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice.

You should consult with your legal counsel to determine what laws and regulations may apply to your circumstances.

Any costs, savings and benefits of any recommendations or programs may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify.

Elavon is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Elavon makes no warranty express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights. To the extent permitted by applicable law, Elavon shall not be liable to a customer or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.

Elavon reserves the right to revise our guidance and any documents already in the public or private domain pending further developments.

About this guidance

Who needs to take action?

This latest in a series of Elavon guides to navigating Payment Services Directive II (PSD2) Secure Customer Authentication (SCA) regulations and mastering transaction optimisation is only intended for merchants and their solution providers operating within the travel-and-hospitality (T&H) payments ecosystem.

This communication builds upon the concepts and recommendations described in a previous Elavon guidance, PSD2 Strong Customer Authentication (SCA) for the Travel & Hospitality Sector.

If you are a merchant operating outside of the T&H payments ecosystem, or if you are a T&H merchant that only accepts sales through secured direct channels, then this advice is not intended for you and no further reading is required.

If you operate within the T&H sector and rely upon bookings made via third parties such as travel-management companies (TMCs), online travel agents (OTAs), other merchants (e.g. an airline facilitating a booking for a hotel or car rental, or a hotel, cruise line or car-rental chain taking a booking on behalf of their franchisee), or if you contract with any other players involved in the booking process that contribute to the processing of payment card transactions, then this update is for you and you will need to take action to get to a compliant and optimised state.

Getting ready for PSD2 SCA compliance

The dates have changed, but the demands have not

PSD2 regulatory enforcement of SCA is widespread across the European Economic Area (EEA) since the passing of the December 2020 deadline. UK enforcement has been delayed until 22 March 2022, however the modified ramp-up commenced as planned on 1 June 2021.

Throughout the EEA and the UK, card issuers will be required to decline all non-SCA-compliant transactions once ramp-up to full adoption concludes in each jurisdiction. All merchants, booking agents, suppliers, acquirers, gateways, and issuing banks or payment service providers must be ready to support SCA.

In a previous guide, we shared with you some of the unique challenges that the introduction of SCA presented to the T&H payments and customer experience ecosystem. We explained what the industry has been doing to address the known 'air gap' in the T&H sector on your behalf. Without the required technical guidance provided by any regulatory authority, you were introduced to the industry-agreed 'interim solution', enabling the continued use of merchant-initiated transactions (MIT) but without 'proof of authentication' until such time as guidance became available and upgrades could commence.

We now have a situation where businesses in the UK and Europe are reliant upon transactions that might originate on infrastructure ordinarily considered as 'beyond the scope of EU regulations'. However, as these transactions form part of the customer sales engagement cycle and therefore require 'proof of authentication' that can only result from SCA being applied 'up front', non-EU (EEA/UK) players and their infrastructure now come into scope and must be engaged in upgrade decisions.

Elavon has continued to work closely with the regulators and card schemes, engaging on T&H task forces with industry stakeholder groups created to bring about 'global solutions for an EU scenario'. Those efforts have resulted in this technical guidance for the ecosystem.

This guidance is being provided for T&H merchants and their solution providers to help you take the necessary steps to comply with the SCA regulation and new rules. Those new rules require all parties to make the necessary changes to enable customers to authenticate their transactions in a way that complies with the underlying regulation.

'Best in class' transaction optimisation can only be achieved when all participants have upgraded their systems to be capable of transmitting authentication data down the chain, as well as receiving authorisation data upstream.

This update provides the specific detail required to satisfy the requirements of participating schemes, card issuers and merchant acquirers, enabling you to bridge the T&H 'air gap' with future-ready technical guidance for compliance to PSD2 SCA, using transaction treatment use-cases supported by card-scheme operating rules and frameworks.

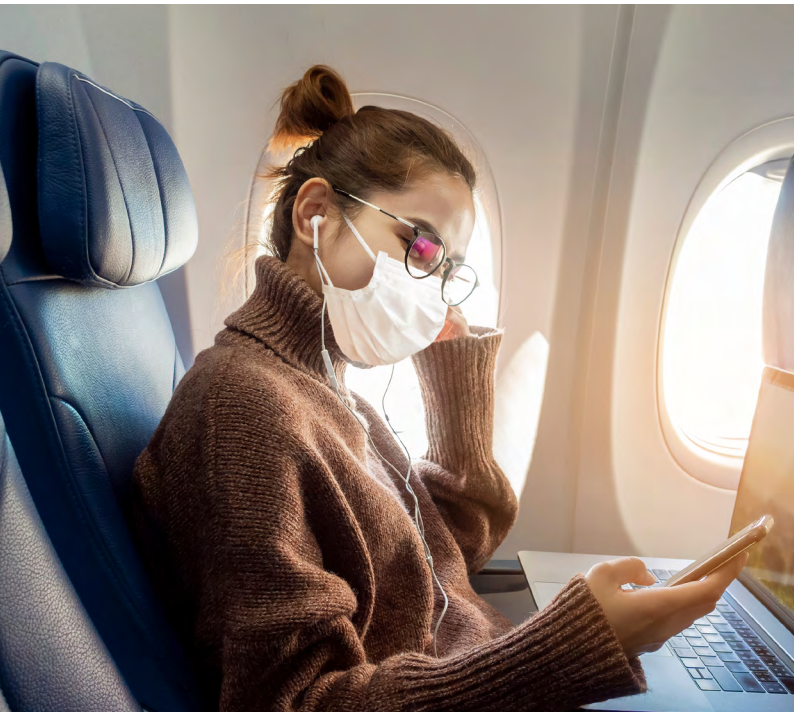
If merchants, booking agents and their solution providers do not act, non-compliant eCommerce card-based payment transactions will be declined unless exempted or determined to be out of scope. In the absence of any industry standard body enabled to provide any guidance or standards on the topic of passing data between 'booking agents' and 'merchants', this guidance will help you reduce the risk of declines when your payments originate from indirect bookings and channels.

PSD2 SCA scope, impacts and implications

Unless a transaction qualifies for an exemption[1] or is out of scope[2] of the regulation, SCA will be required for all online (website or app) card payments. For the T&H sector, this includes:

- Direct sales[3] made by the T&H merchant[4] and
- Indirect sales[5] when T&H bookings are made through an independent third party.

Merchants will no longer be able to send payment transactions that originated by eCommerce/mCommerce card-not-present (CNP) bookings as MOTO (mail order/telephone order) or simple CNP transactions without authentication data (e.g. airline sales) or through manual PAN (primary account number) key entry, using point-of-sale solutions (e.g. hotels, car rental or other supplementary sales on a travel booking).



For MITs, out-of-scope payments are initiated by the merchant based on pre-existing authority and the cardholder is not involved 'in-session' when they originate. However, the action of granting authority whereby the cardholder agrees to pay any fees associated with a booking is caught by SCA requirements and must be authenticated. When bookings and purchases are made through an online or mobile booking channel, authentication will generally be performed using EMV 3DS[6].

(1) Please refer to the 'Regulatory Technical Standards on strong customer authentication and common and secure open standards of communication' for more information about SCA exceptions and exemptions or see our previous T&H guide here or go to our website for more PSD2 SCA information.

(2) Transactions can be considered out of scope if 1) performed with an anonymous card (e.g. prepaid card); 2) booking is done though mail or telephone order; 3) either (or both) the issuer of the card or the merchant's acquirer is located outside of the EEA or 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.

(3) Direct sales are remote eCommerce bookings and transactions made on your own infrastructure which may include websites and mobile apps, all of which must be secured for SCA, typically using EMV 3DS. Proof of those authentications must also be passed through your systems to enable the establishment of MIT agreements with the cardholder. However, this document only refers to third party bookings via independent agents – indirect sales.

(4) The word 'merchant' in this document is used to designate any T&H supplier when it processes transactions as a merchant. Note that when a booking agent collects funds as a 'merchant of record' in an authorisation on a travel booking, the booking agent becomes a merchant as well.

(5) Indirect sales rely upon bookings made via third parties such as travel-management companies, online travel agents, other merchants (e.g. an airline facilitating a booking for a hotel or car rental, or a hotel, cruise line or car-rental chain taking a booking on behalf of their franchisee) and includes your contracts – with every player involved in the booking process that contributes to the processing of payment-card transactions. For some, this will include other related service providers such as insurance providers, metasearch engines, tour operators and more.

(6) We recommend you support EMV 3DS V2.2 to ensure the best cardholder interface experience and to ensure that all T&H use cases can be supported for all payment brands.

Advance deposits, balance payments and cancellation fees processed[7] by T&H merchants (or global distribution systems [GDS] for airline ticket sales) may all qualify as MITs. Unless the transaction can otherwise qualify for any other exemption or is out of scope, authentication will be required and the authentication data and/or reference to it must be present in each MIT.

Merchants must upgrade to solutions enabling them to send payment authorisation requests with the appropriate authentication data gathered during the booking process. The changes required to provide proof of authentication may impact the software, platforms and services provided to you from solution providers involved in the collection, transfer, processing and/or storage of T&H bookings and associated payment information on your behalf. These could include Global Distribution Systems (GDS), Customer Reservation Systems (CRS), Property Management Systems (PMS), online corporate booking tools, travel content aggregators, channel managers, the International Air Transport Association Billing and Settlement Plan (IATA BSP), NDC[8] aggregators and many other intermediaries involved in the T&H payments cycle.

CNP transactions without authentication data or without an applicable exemption will be subject to declines once the ramp-ups complete on the enforcement deadline dates.

(7) Also applies to full payment at end of stay, end of rental (and delayed charges) if check-in is performed without cardholder present/authentication.

(8) 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).

The T&H journey towards SCA compliance: the story so far

In our previous communication for T&H, we outlined the key principles of, and challenges introduced by, the need for SCA across all card-payment types in both direct and indirect sales channels.

The absence of a regulatory standards body to produce technical guidance required to process MITs originating in remote and indirect/independent sales channels, aligned to the fast-approaching deadlines for compliance, put these transactions at immediate risk of failure. Merchants' inability to provide 'proof of authentication' for card issuers' approval when third-party-booked authorisation requests were made meant the risk of unnecessary step-up requests for EMV 3DS from issuers when the cardholder was no longer 'in session' and could not respond – resulting in hard declines and lost sales.

A highly complex ecosystem with many intermediaries in the booking and payments chain complicates payment-chain upgrades for the global industry already. Without technical guidance and standards, and with no stakeholders wanting these transaction types to fail and although 'MIT with proof of authentication' is agreed by all to be the best in class and compliant approach, an interim solution that enabled 'MIT without proof of authentication' was called for until such time as the technical, operational and contractual changes can be completed.

As your acquirer, we enabled you to use the interim solution by updating our contracts with you and authorising you to use the existing PSD2 SCA 'out of scope' condition flags of MOTO and MIT (without proof of authentication). This was to give these transaction types the best possible chance of success.

We also described for you the urgent need to decide upon an engagement model with all of your independent third-party agents that service you with bookings and reservations – indirect sales.

The route to full compliance and changes to data flows required are now dependent upon the choices you make in these channels. There may be other compliant solutions available. However, we described for you three generic models in common use today.

Your booking agent authentication options reviewed

Option 1

Agent has no EMV 3DS SCA capability/agent takes no payments

The booking agent may send booking details directly to an eMerchant. 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.

Option 2

Agent authenticates via EMV 3DS and collects all payments required on merchant's behalf

The booking agent may perform authentication with the cardholder and collect ALL required payments on behalf of the travel or hospitality supplier (e.g. at booking, on a pre-agreed date or at an agreed time in the event of a cancellation or 'no show' charge being applied).

Option 3

Agent authenticates and all payments are to be processed by merchant

The booking agent may perform SCA and pass authentication data and other transactional data to the merchant, enabling the merchant to request/perform MIT to collect payment as agreed with the customer.

- This may or may not include the booking agent collecting some funds at the point of booking. Either way, authentication-related data must be passed to the 'merchant of record' as the data will be required to process future payments (e.g. MITs to effect a balance payment or full payment associated to a check-in performed without face-to-face interaction).

The remainder of this document provides guidance on the data that must be passed between booking agents and merchants to meet compliance, in cases where Option 3 is the chosen solution. The technical guidance following references all of the relevant data fields that you will require to meet compliance, as well as providing you the foundation for optimising your authentication and authorisation flows for maximum approval rates when indirect sales feature.

Elavon

Speak to your Customer Services Team for more details

UK 0345 850 0195
IRE 1850 202 120

elavon.co.uk
elavon.ie

Technical guidance for Option 3

In any indirect sales situation where a merchant intends to process payments themselves and requests that the booking agent performs authentication on their behalf (Option 3 above), operational readiness and full compliance is achieved with the use of supplemental data. This is captured by the booking agent, passed to the merchant and used to establish MIT consent from the cardholder.

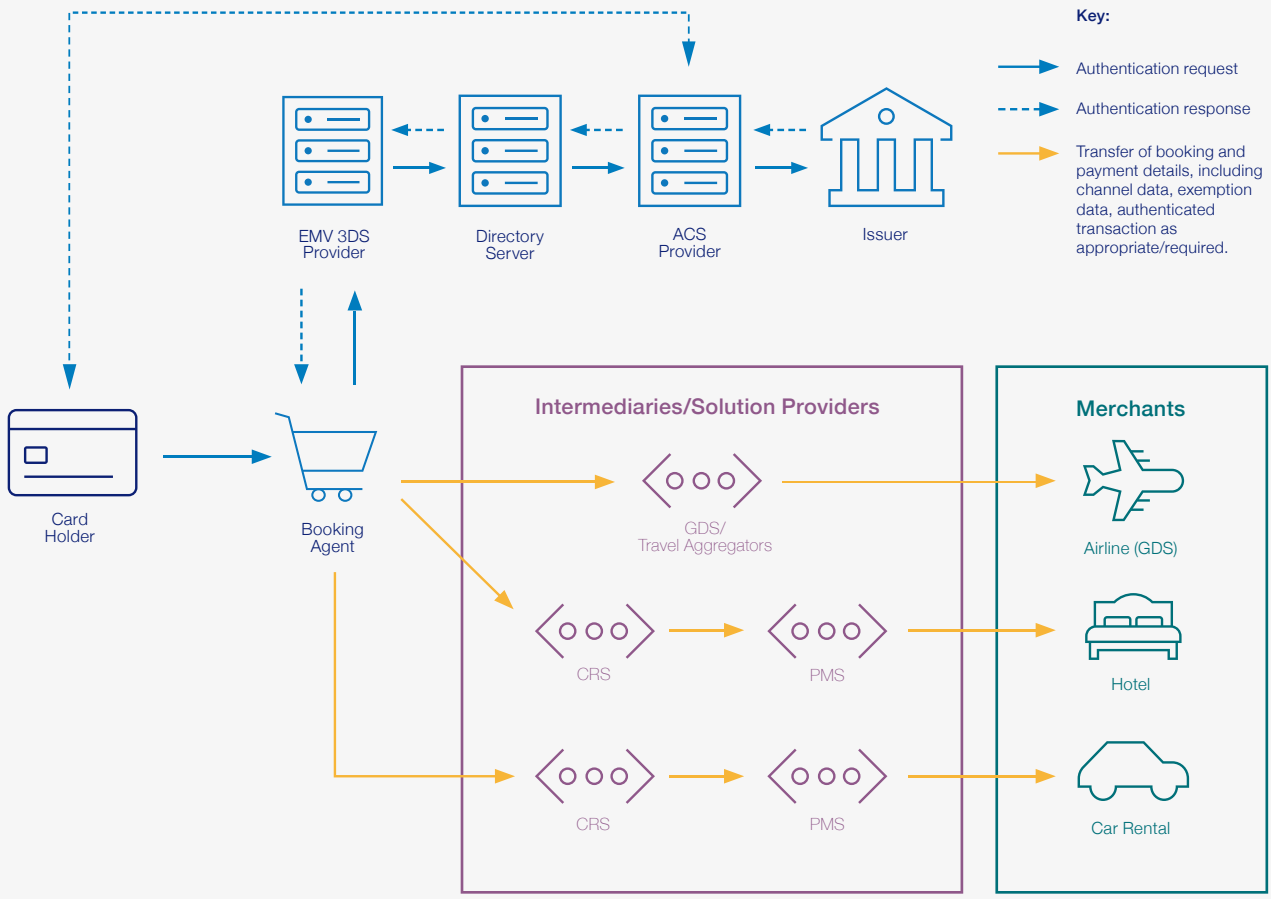
Merchants must ensure that mechanisms are in place that enable authentication data to be sent and/or received between themselves and their booking agents. This may involve intermediaries and merchants upgrading their systems to enable transfer of authentication data required to receive and submit payment authorisations, as well as other associated data (e.g. booking information).

An authentication code, Electronic Commerce Indicator (ECI) value and other associated information is generated by the authentication provider and provided to the booking agent when the authentication of a remote indirect booking completes.

This ‘proof of authentication’ must be sent to the merchant, together with information relating to the context of the transaction to enable the merchant to submit subsequent payment authorisation requests. In cases where a booking agent processes a 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 in the remainder of this document. This means that all intermediaries and solution providers involved in passing booking and payments details between the booking agent and merchant must upgrade their systems to pass the required data, as illustrated in Figure 1:

Figure 1



Step 1

The booking agent must perform authentication (unless an exemption can be used, or the transaction is out of scope).

Step 2

Solution providers, in passing booking and payment details between a 'booking agent' and a T&H merchant, must upgrade their systems to pass the required data.

Step 3

Merchants must upgrade their booking/ payment system to recieve the required authentication and associated data and include them in their payment transactions.

Updates required from booking agents, merchants and their solution providers

The following section describes the actions that booking agents, solution providers and intermediaries must take to pass data between each other, in order to ensure merchants can process payment authorisation requests in a compliant manner.

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:

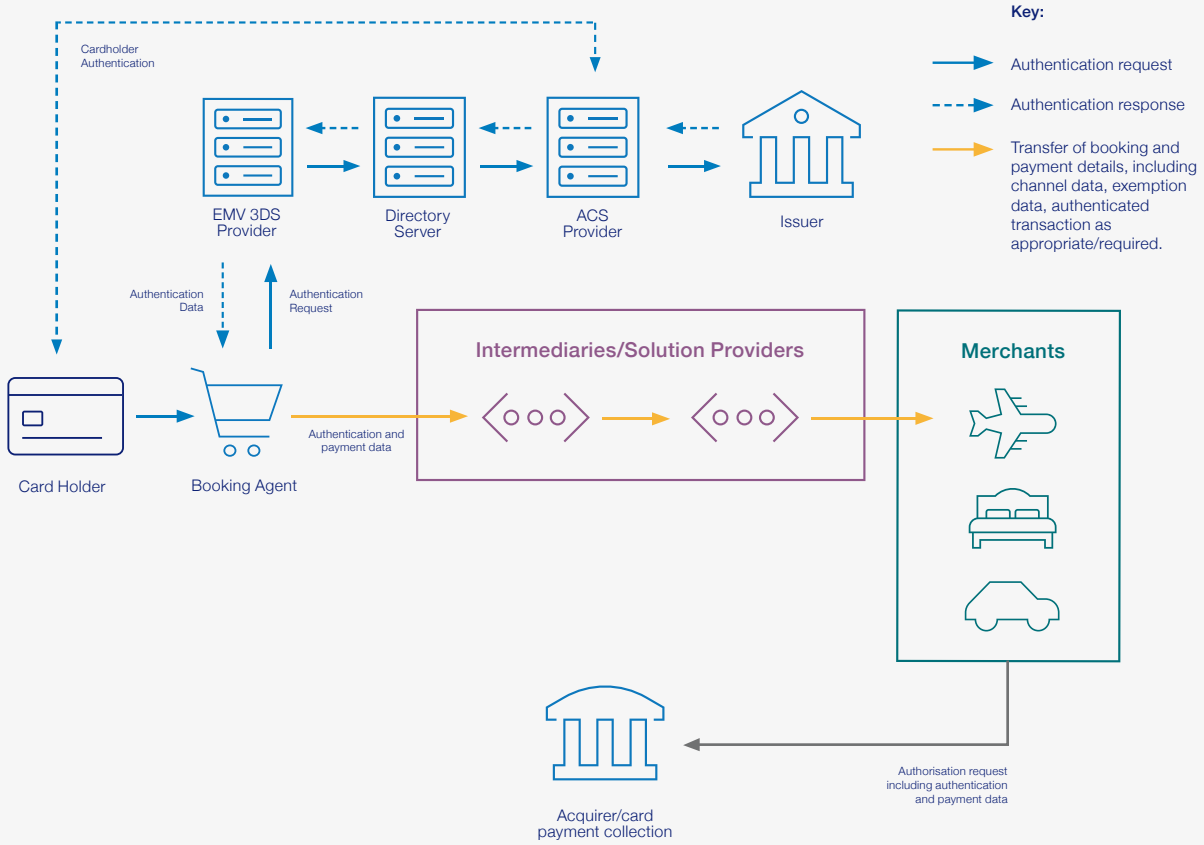
Scenario A

The booking agent authenticates the cardholder, and the supplier of the T&H service collects the payment as the 'merchant of record'.

In this scenario, the booking agent must send the relevant authentication data to the merchant either directly or through intermediaries to enable the merchant (or GDS, for airline ticket sales) to request payment authorisation and collect funds associated with the booking, or to set up the authenticated MIT agreement for a later authorisation[9].

(9) 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.

Scenario A



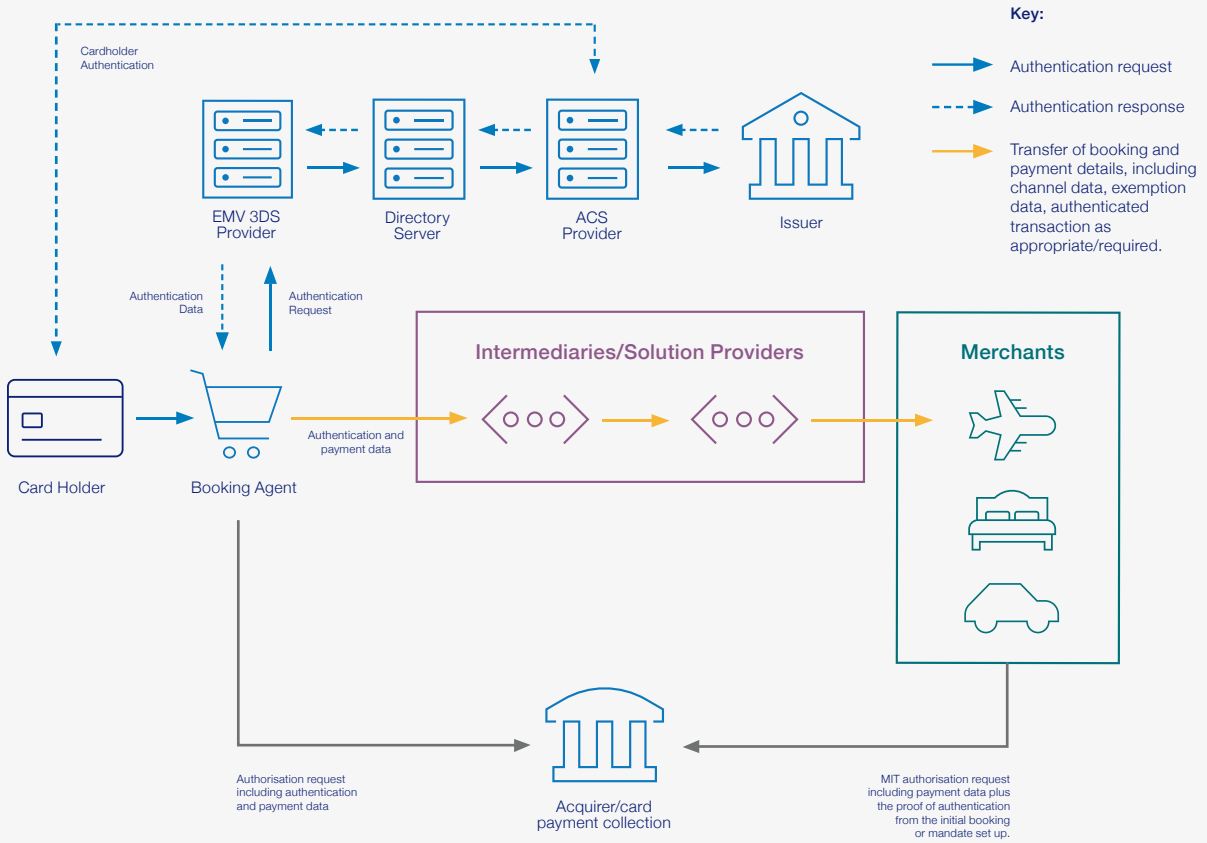
Scenario B

Booking agent authenticates the cardholder and processes an authorisation to 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 collect funds at a later time.

Following authentication, the booking agent requests payment authorisation to collect funds associated to a booking and/or informs the respective card issuer of the setup of an MIT agreement[10]. 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.

(10) Where no funds are due at the time of 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.

Scenario B

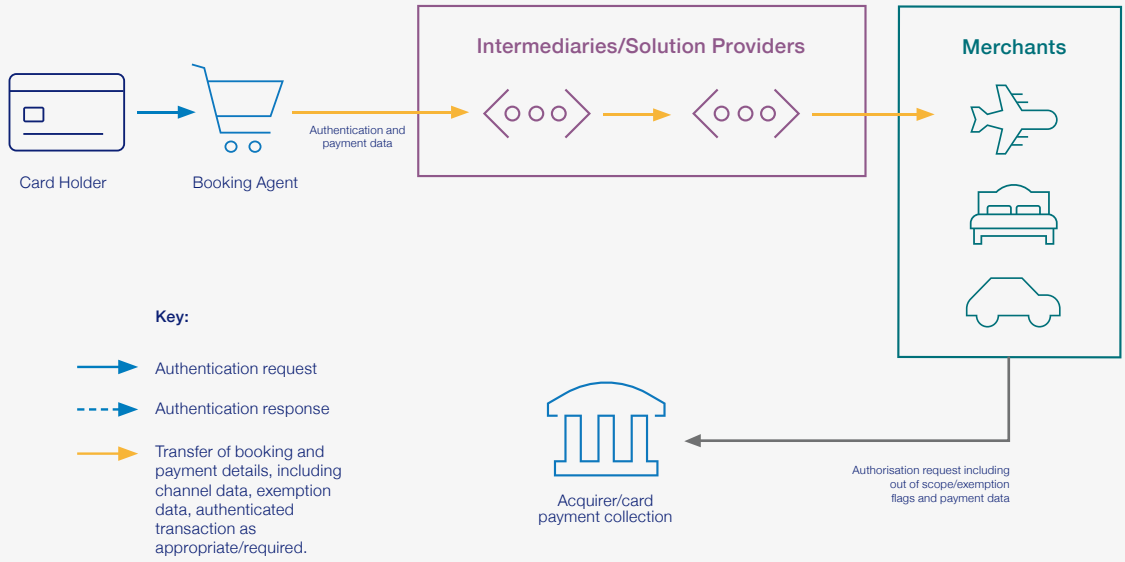


Scenario C

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 T&H service collects the payment.

In this scenario, the data relative to the out of scope or exempt payment type must be passed onwards to the T&H merchant (or GDS, for airline ticket sales) along with the other payment data for the T&H supplier to perform their own authorisation request as the merchant of record[11].

Scenario C



Note that 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 the 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 TMCs and OBTs may qualify for the exemption.

(11) This scenario also covers instances where there is an authentication outage in the acceptance flow and authentication could not be performed.

Data requirements

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 Data Table 1 which follows on Page 21.

Booking agents must ensure[12]:

- 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 Data Table 1.
- Data elements marked as **'RM'** (Recommended) are recommended to be sent if they are available – as per the 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.

- Solution providers will need to be ready to receive *any* of the data elements detailed in Data 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. The data requirements should be discussed with the travel merchants for whom booking agents perform services for, to ensure all requirements meet the PSP's guidance.

- 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 data from the booking agents to merchants is completed as soon as possible. Merchants must work with their solution providers who, in turn, must work with other upstream and downstream providers with whom they exchange payment transaction data to agree the earliest possible integration timelines.

(12) Booking agents should always discuss with their merchants/PSP to ensure they can pass the data required by schemes at any point in time. The table below recommends that some fields are reserved for future use so that any new data requirements can be added with ease.

- 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** have been made available by the payment schemes to ensure that transactions are not declined due to lack of authentication data/or reference to it where this cannot yet be provided.

- Merchants and solution providers should take note, however, that these situations 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 compliant solutions to merchants.

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

Data Table 1 (see next page) provides guidelines on the specific authentication and associated payment data that solution providers and intermediaries should receive and pass to merchants, following an indirect booking. This is based on required data for processing PSD2 SCA-compliant transactions with major card brands (MasterCard, Visa and American Express) as of the time of publication.

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

In the absence of any other specification, this document is provided as an indication of 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 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 PCI3-DS) as well as maintaining General Data Protection Regulation and PSD2 compliance throughout.

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 table 1

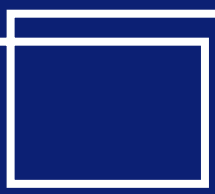
Data	Field Name	Type and Length	Required (R) Conditional (C) Recommended (RM)	Payment Scenarios	Additional Information
1	Card number or Token Number	30 numeric	R	A,B,C	Either a card number or a token number is provided, not both. (A token number is formatted exactly as a card number)
2	Card Brand	25 alphanumeric	RM	A,B,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,B,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. This value is required in scenario C when the T&H supplier is requesting authorisation for a CIT being processed to set up an MIT that will subsequently be collected by the T&H supplier. This value cannot be stored so the T&H supplier must ensure that it processes the CIT using this value as soon as it is received. The value is not needed if authorisation is for a CIT to set up an MIT on behalf of the T&H supplier and is being requested by the booking agent rather than the T&H supplier.
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.

Data	Field Name	Type and Length	Required (R) Conditional (C) Recommended (RM)	Payment Scenarios	Additional Information
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,B,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. This value is required in scenario C when a T&H supplier is requesting authorisation for a CIT being processed to set up an MIT that will subsequently be collected by the T&H supplier and when the transaction may qualify for the SCP exemption. The value is not needed if authorisation is for a CIT to set up a MIT on behalf of the T&H supplier and is being requested by the booking agent rather than the T&H supplier.
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"			
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"			
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"			

Data	Field Name	Type and Length	Required (R) Conditional (C) Recommended (RM)	Payment Scenarios	Additional Information
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"			
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	C	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. Note that Visa only allows the booking agent to set up the MIT on behalf of the T&H supplier (i.e. the only scenario where the Tran ID would need to be passed) when the booking agent is the corporate head office of the brand under which the supplier/merchant is operating as a branded franchisee. In all other cases, the T&H supplier will need to set up its own MIT agreement and therefore it is the authenticator.
10	Merchant Name used by authenticator in authentication request	40 alphanumeric characters	C – to be present if requested by the scheme	A,B,C	Not requested by Visa.
11	3-DS 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, B	The type and length are as per EMV 3-DS 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. This value is required in scenario C when a T&H supplier is requesting authorisation for a CIT being processed to set up a MIT that will subsequently be collected by the T&H supplier and when an authentication value has been obtained for this purpose. The value is not needed if authorisation is for a CIT to set up a MIT on behalf of the T&H supplier and is being requested by the booking agent rather than the T&H supplier.
12	**Authentication Value for Tokens (e.g. TAVV)**	**28 characters. A 20-byte value that has been Base64 encoded, giving a 28-byte result**	**C - to be present if required by the scheme for token transactions AND if transactions indicated as EC in data element 5.3**	**A,B**	**Required only for Visa at this time.** **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 3-DS and have both a CAVV and a TAVV. Booking agents will need to pass on the data they receive.** **This value is required in scenario C when a T&H supplier is requesting authorisation for a CIT being processed to set up a MIT that will subsequently be collected by the T&H supplier and when an authentication value has been obtained for this purpose. The value is not needed if authorisation is for a CIT to set up a MIT on behalf of the T&H supplier and is being requested by the booking agent rather than the T&H supplier.**

Data	Field Name	Type and Length	Required (R) Conditional (C) Recommended (RM)	Payment Scenarios	Additional Information
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,B	Value should be populated as received in authentication response. Values may be different by payment scheme.
14	3-DS transaction ID Value returned by the 3-DS Directory Server	3-DS V1 will provide XID value (XID not required for MasterCard) 3-DS V2 will provide DS Transaction ID Amex: 20 Bytes unsigned binary MasterCard: 36 characters from EMV 3-DS are carried as such into an ISO8583 ans-36 field	C - to be present if 3-DS authentication was carried out and if required by scheme in transaction data	A,B	Not required by Visa at this time.
15	3-DS Program Protocol version	3 alphanumeric (no dots in between values)	C - to be present if required by the scheme	A,B	This may be required in authorisation request for certain schemes. Not required by Visa at this time (this value is included in the authentication value, i.e. in CAVV Version 7.)
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 not applicable for the country			
16.8	Street 1	Max 50 characters			
16.9	Street 2	Max 50 characters			
16.10	Street 3	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-3-DS 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.

Data	Field Name	Type and Length	Required (R) Conditional (C) Recommended (RM)	Payment Scenarios	Additional Information
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-3-DS 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 authentication issues as they may be created from time to time	2 alphanumeric			
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 3-DS 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



Elavon®