Implementing Strong Customer Authentication (SCA) for Travel & Hospitality

June 2021

Version 2.0
24 June 2021

Contents

Important Information

Disclaimer: Case studies, comparisons, 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.

As a new regulatory framework in an evolving ecosystem, the requirements for SCA still need to be refined for some use cases. This paper represents Visa's evolving 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 competent authorities' guidance and clarifications. Visa reserves the right to revise this guide pending further regulatory developments.

This guide is also not intended to ensure or guarantee compliance with regulatory requirements. Payment Service Providers are encouraged to seek the advice of a competent professional where such advice is required.

This document is not part of the Visa Rules. In the event of any conflict between any content in this document, any document referenced herein, any exhibit to this document, or any communications concerning this document, and any content in the Visa Rules, the Visa Rules shall govern and control.

Note on references to EMV 3DS: When in this document we refer to EMV 3DS, this is a generic reference to the second generation of 3-D Secure and does not reference a specific version of the EMVCo specification. Version 2.1 of the specification is referred to as EMV 3DS 2.1 and version 2.2 is referred to as EMV 3DS 2.2. Visa rules do not preclude Issuers and Acquirers agreeing alternative means of performing SCA.

Note on references to "SCA" and "authentication": The term "SCA" is used in this guide refer to the application of a Strong Customer Authentication challenge when such a challenge is required. The term "authentication" is used to refer more generically to the authentication process flow through which an agent or merchant requests authentication and which may result in either the application of an SCA challenge or of an exemption.

Examples in this document show transactions processed through VisaNet. Visa supports the use of third party processors. Contact your Visa Representative to learn more.

1. Introduction

PSD2 requires that PSPs (Issuers and Acquirers) apply Strong Customer Authentication (SCA) is applied to all electronic payments - including proximity and remote payments - within the European Economic Area (EEA) and the UK.

The requirement to apply SCA came into force on 14 September 2019. In relation to e-commerce card payment transactions, the European Banking Authority (EBA) has recognised the need for a delay in enforcement to allow time for all parties in the payments ecosystem to fully implement SCA, setting a deadline of 31 December 2020 by which time the period of supervisory flexibility was to have ended. The SCA migration plans of PSPs, including the implementation and testing by merchants should also have been completed by 31 December 2020. While the majority of National Competent Authorities (NCAs) have now aligned with the EBA's guidance, PSPs should check with NCAs for enforcement timescales in their respective markets since in some jurisdictions local regulators may be exercising some short term flexibility in enforcement during at least the initial part of 2021. As regards the UK, the Financial Conduct Authority (FCA) will start to enforce the SCA mandate regulation which transposes PSD2 into UK law from 14 September 2021 in relation to e-commerce (subject to compliance with phased implementation plans).

Merchants, booking agents, and intermediaries in the Travel and Hospitality (T&H) sector need to ensure that SCA can be applied to all transactions that are in scope of the regulation. Merchants need to note that any transactions submitted after the enforcement date without SCA or without correct exemption or out of scope indicators are at risk of being declined by Issuers. This includes all card not present (CNP) and face to face transactions, including transactions that are initiated by a merchant during the course of a hotel stay or car rental.

Visa recognises that the application of SCA brings specific challenges to the T&H sector due to the complexity of some booking processes and business models, and the reliance on legacy booking, payment and settlement systems and processes that may not currently support the passing of required authentication data. As a result, Visa has been working with T&H sector and payments industry stakeholders, relevant industry associations and regulators to identify interim and longer-term solutions that will enable transactions to be processed as required by the regulation.

This guide provides specific guidance to T&H merchants, booking agents and intermediaries and to Issuers, Acquirers and gateways on:

- The application of SCA to sector specific booking and payment scenarios
- Interim and longer-term solutions to ensuring that SCA can be applied where required and out of scope transactions and exemptions can be identified and processed correctly.

Some specific transaction types are "out of scope" of SCA and do not require the application of SCA, subject to certain qualifying conditions being met. Furthermore, the SCA mandate is complemented by some limited exemptions that aim to support a frictionless customer experience when a transaction risk is low. This guide makes references to circumstances where transactions may be out of scope or may qualify for the application of exemptions. For more detailed information on the definition and identification of out of scope transactions and the qualification for, application and indication of exemptions please refer *to PSD2 SCA for Remote Electronic Transactions Implementation Guide*.

This guide is not intended to provide legal advice nor to ensure or guarantee compliance with regulatory requirements. Payment Service Providers merchants, booking agents and intermediaries are encouraged to seek the advice of a competent professional where such advice is required.

2. The Travel & Hospitality context for PSD2 SCA

This section summaries key terminology and assumptions used throughout the guide, specifically the roles of the T&H ecosystem participants and generic processes used in the booking of T&H services and collection of payment for those services.

2.1 Travel & Hospitality ecosystem participants

T&H bookings and associated transaction processes commonly involve multiple parties. The terminology in Table 1 below is used to describe these parties:

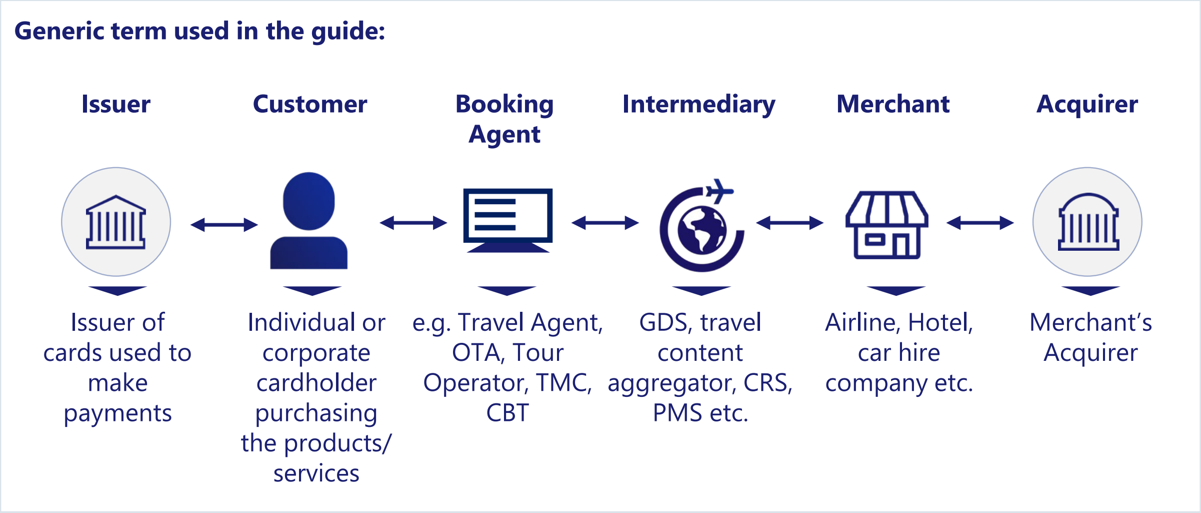
Table 1: Ecosystem participant definitions

Party	Definition
Customer	The individual or corporate customer that is the ultimate payer for the product or service being purchased.
Merchants	A party that collects a card based payment from an end customer or a booking agent. The merchant is always the party that requests payment authorization but may or may not be the party that requests authentication or that supplies the service. Booking agents and suppliers may both act as merchants.
Booking Agents	The party taking a booking on behalf of an end customer and one or more suppliers. Booking agents include: • Online Travel Agents (OTA) • Physical (bricks and mortar) travel agents, including those with an online booking channel • Travel Management Companies (TMCs) • 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 car 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.

	Booking agents may act as the merchant where they collect payment for all or part of a booking from the end customer on behalf of the supplier(s).
T&H Suppliers	Suppliers are providers of Travel and Hospitality services to end customers. Examples include: • Airlines • Hotel operators • Car rental companies • Providers of ancillary services such as airport transfers, sightseeing trips etc. Suppliers act as merchants when: • They collect payment from the end customer as part of a direct or indirect booking and payment process • They collect a B2B supplier payment from a booking agent that has collected payment from a customer. This supplier payment, when made by card is usually made using a commercial virtual card.
Intermediaries	Intermediaries are 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 • Travel content aggregators • Channel managers • Global Distributions Systems (GDS) • NDC[1] aggregators • IATA BSP • Software platform and payment providers to any of the above Intermediaries may pass booking, payment and authentication data between booking agents and suppliers and may process payments on behalf of suppliers.

[1] 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.

Figure 1: Generic terms for stakeholders used in this guide



Generic term used in the guide:

Issuer — Issuer of cards used to make payments

Customer — Individual or corporate cardholder purchasing the products/ services

Booking Agent — e.g. Travel Agent, OTA, Tour Operator, TMC, CBT

Intermediary — GDS, travel content aggregator, CRS, PMS etc.

Merchant — Airline, Hotel, car hire company etc.

Acquirer — Merchant's Acquirer

2.2 Direct and indirect bookings

- **Direct bookings** are defined as bookings in which the customer makes the booking directly with the travel or hospitality (T&H) supplier via the supplier's own website (or reservation desk) and where the T&H supplier is the merchant collecting payment. An example would be booking a flight directly via an airline's own website.
- **Indirect bookings** are defined as bookings made via a booking agent acting on behalf of a supplier. Examples include a booking for a flight, or a hotel room made via an OTA or when a hotel or car rental booking takes place on the corporate website of the company brand but where the transaction is processed via the franchisee as the merchant.

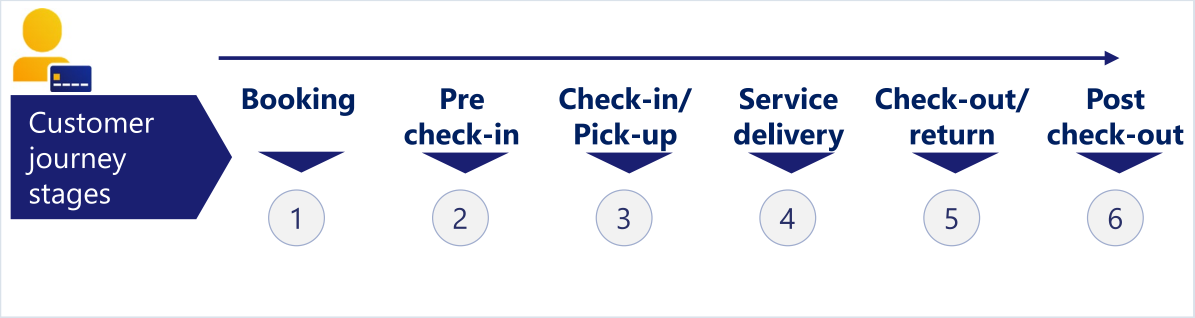
2.3 Customer journey and payment stages

There are a number of stages in the travel and hospitality booking and delivery customer journey at which SCA may be required and/or a payment may be taken. These stages are summarised in Figure 2 below and referred to throughout the guidance. The actual points at which authentication and authorization are requested and which party is responsible depends upon:

- The specific payment use case
- Whether the booking is direct or indirect
- The parties involved in processing the booking and payment transaction
- The business model adopted between the parties
- The terms and conditions of booking agreed with the customer

Specific scenarios and authentication and authorization flow stages for key use cases are described and mapped on to the customer journey in section 5

Figure 2: Generic customer journey & payment stages



2.4 Face to Face, remote and MOTO payments

Depending on the payment use case and stage in the journey a payment transaction may be:

- **Face to face:** for example in a bricks and mortar travel agent, at an airline booking desk, on check in or check out of a hotel, or collection or return of a rental vehicle. Where required, authentication must be undertaken using chip and PIN (or other valid cardholder verification method such as biometrics in the case of mobile payments).The contactless payment exemption may apply to some face to face payments, where they qualify, however the exemption may not be used for transactions that set up an MIT agreement, or when the cumulative contactless transaction count or value limit since last application of SCA is exceeded [2].
- **Remote:** for example online prepayments made by customers booking through an OTA or supplier website. Remote payments include Customer Initiated Transactions (CITs) and Merchant Initiated Transactions (MITs) as described in section 2.5 below. SCA must be applied for all remote transactions unless the transaction is out of Scope of SCA or an exemption can be applied. For more information of identifying and indicating out of scope transactions and the application of exemptions please refer to Appendix A.1 and *PSD2 SCA for Remote Electronic Transactions Implementation Guide*.
- **MOTO:** Transactions that are the result of booking via a mail order/telephone order channel only. These transactions are out of scope of the PSD2 SCA regulation and no SCA is required. It has been common practice in the T&H sector to manually key enter and flag transactions as MOTO even when they originated from e-commerce booking. This practice is no longer permitted with the enforcement of PSD2 SCA. See section 3.2.2 below for more detail.

2.5 MITs & CITs

2.5.1 Merchant Initiated Transactions (MITs)

A Merchant Initiated Transaction (MIT) is a transaction, or series of transactions, of a fixed or variable amount and fixed or variable interval, governed by an agreement between the

[2] For more information on the application of the contactless exemption, please refer to Visa Contactless and Card Present PSD2 SCA: A Guide to Implementation.

cardholder and merchant that, once agreed, allows the merchant to initiate subsequent payments without any action from the cardholder.

MITs are out of scope of SCA, however in order for a transaction to be processed as an MIT without SCA being applied a number of conditions need to be met. These include:

- The customer must be presented with the terms and conditions governing the MIT and SCA must be applied (i.e. no exemption can be used, except the secure corporate payment (SCP) exemption, where applicable) when the MIT agreement with the cardholder is set up through a remote electronic transaction[3].
- Transactions can only be considered MITs when the cardholder is not available to (i) initiate; or (ii) authenticate the transaction.

The Visa MIT Framework defines and identifies eight different types of MITs. Details of these may be found in the *PSD2 SCA for Remote Electronic Transactions Implementation Guide*.

MITs in the T&H sector (and their associated MIT type under the Visa MIT Framework) include transactions for:

- One or more prepayment(s) or balance payment(s) collected after booking but prior to check-in/pick-up (MIT – Installment/Prepayment)
- No show/cancellation fee (MIT- No Show)
- Initial estimated authorization to block funds at check in when the customer is not present (MIT - Reauthorization)
- Additional authorization to block additional funds for services consumed during a stay/rental (which can be processed throughout the stay/rental and at end of stay/rental when the customer is not present) (MIT- Incremental)
- Authorization to block funds when the authorization validity limit set by Visa expires but the when the fulfilment of the original order/service is not yet completed, e.g. for extended stay (MIT – Reauthorization).
- Charges applied after checkout or vehicle return, such as minibar usage, or hire car refueling costs after the payment for the service rendered had already been completed. (MIT- Delayed Charges)

For more information on MITs and the Visa MIT framework that must be used to identify and process MITs please refer to section 3.4 and to *PSD2 SCA for Remote Electronic Transactions Implementation Guide*.

2.5.2 Cardholder-initiated transactions (CITs)

A cardholder-initiated transaction (CIT) is any transaction that is not an MIT as defined in section 2.5.1 and includes any transaction where the cardholder is available to initiate or authenticate the transaction. Authentication is required for all CITs, unless the transaction qualifies for an exemption or is otherwise out of scope of SCA. Note that exemptions cannot

[3] Except if the transaction is out of scope, for example when the agreement is set up via the MOTO channel, SCA is not required as MOTO transactions are out of scope of SCA.

be used when the CIT is performed to set up an MIT agreement, except if the transaction qualifies for the SCP exemption.

Depending on whether a CIT is in scope and how SCA is being performed or exempted, the merchant must include the required out of scope or exemption indicators and authentication data with the authorization message as defined in the *PSD2 SCA for Remote Electronic Transactions Implementation Guide*.

Table 2: Summary of Transactions types and SCA requirements

Transaction type	Description	SCA required ?	
CIT	Customer Initiated Transaction. Transaction taking place at booking to either • Collect immediate payment, or	✓	unless transaction is out of scope or qualifies for an exemption.
	• Collect immediate payment and set up a mandate for the merchant to initiate subsequent MITs, or	✓	no exemption can be used in a CIT that is performed to set up an MIT mandate, except when the transaction qualifies for the SCP exemption
	• Set up a mandate for the merchant to initiate one or several payment transactions later (MITs).		
MIT	Subsequent Merchant Initiated Transaction as defined in section 2.5.1	✗	

3. Key principles for the application of SCA to Travel & Hospitality payments

The following principles apply to the authentication and authorization of all T&H payment transactions:

1. Authentication must be requested on all in scope transactions at time of booking
2. An Authorization request must take place within 72 hours of booking, with proof of authentication (or be marked out of scope as appropriate)
3. The amount authenticated and authorized must be for the amount due at booking.
4. Any payments taken after booking which require merchants to initiate payments at a time when the cardholder is no longer available to perform authentication can be processed as MITs. This applies to:
   - Payments taken by an agent on behalf of a T&H supplier, or by the T&H supplier, after booking but before check-in. These must be authenticated at booking, and all applicable terms and conditions that govern the collection of the MITs must be presented before authentication, including when the authentication is requested by the booking agent
   - Payments taken by the T&H supplier after check-in where authentication may be requested by the T&H supplier either:
     - Through a face to face transaction at check-in, using Chip & PIN or other appropriate cardholder verification method in the case of mobile payments, or
     - Through EMV 3DS in the case of an "express" or "keyless" check-in facilitated through the T&H supplier(s) website or mobile app
5. Booking agents and merchants need to mutually agree which party will request authentication depending on the payment use case and business model adopted
6. Bookings for corporate purposes that are initiated electronically through dedicated payment processes or protocols that are not available to consumers, may qualify for application, by the Issuer, of the secure corporate payment (SCP) exemption, subject to the view of local regulators and the payment being made with an eligible card

These principles are further explained below:

3.1 Principle 1: Authentication must be requested at booking for any transaction that is in scope

Authentication must be requested at booking to cover any in scope payment that is due to be taken either at booking or at any subsequent time when the customer may not be available to authenticate, (for example prior to check in). This includes[4]:

- Payment of a deposit or full amount at the time of booking (CIT)
- Any (initial or subsequent) prepayments not due at booking but later and before the customer checks-in (MIT)
- Guaranteed reservation/cancellation fee through an MIT in case of No Show
- Initial authorization at a card not present check in and any incremental CNP authorization before/at check-out (both MITs)

3.1.1 Authentication requirements/considerations

The following requirements/considerations also apply at the time of booking and authentication:

1. The terms & conditions of the booking must be clearly presented to the customer before authentication[5]. These must include at least:
    - The final amount that will be collected, or
    - How the final amount will be calculated if the final amount is not known at time of booking; and
    - When the amounts will be collected and by whom
2. Authentication may be requested by a booking agent (see other options in section 4), even if that booking agent is not the merchant, although please note that in this case the booking agent will need to pass evidence of authentication to the merchant prior to the merchant requesting authorization
3. Face to face booking transactions must be authenticated using chip & PIN or contactless with cardholder verification
4. E-commerce booking transactions will, in most cases, be authenticated through EMV 3DS
5. Exemptions may be applied to transactions that qualify, unless an agreement to process subsequent transactions as MITs is being set up, in which case SCA is required.

[4] This list is not exhaustive, for full list, refer to section 3.4.1

[5] Note: In the case of an indirect booking if the booking agent is unable to present the T&Cs for any payment that may be collected because the final terms of each payment are not known, the booking agent will only be able to request authentication for a no show payment at the time of booking. Authentication for all other subsequent payments collected by the merchant(s) will need to be requested by the merchant(s) at check in, for example by a chip and PIN or mobile biometric authentication in the case of a F2F check-in or EMV 3DS on the merchant’s mobile app in the case of an “express” /”keyless check-in.

If a merchant identifies that the transaction qualifies for an exemption and would like the exemption to be applied, it must submit the transaction via EMV 3DS or direct to authorization with the appropriate exemption indicator.

- Note that exemptions can only be applied by an Acquirer and a booking agent that is not the merchant is unlikely to know whether the merchant's Acquirer is supportive of an exemption. The exception is when the booking agent is originating the transaction in a qualifying secure corporate environment and the SCP exemption applies.

6. If any subsequent payments are to take the form of MITs, exemptions cannot be applied to the CIT processed at time of booking to set up the MIT and an SCA challenge is required. For this CIT, the challenge indicator in EMV 3DS must be set to 04. The only exception to this is if the transaction qualifies for the SCP exemption or if the CIT processed to set up the MIT agreement is made via the MOTO channel or is otherwise out of scope.
7. If the booking agent/merchant does not identify that an exemption may apply, it must submit the transaction via EMV 3DS for application of SCA and then request authorization providing appropriate proof of authentication in the authorization request
8. Authentication must be requested for all in scope payments even when made using a stored credential, for example a card held on file as part of a loyalty or VIP customer scheme, unless the transaction is an MIT that has been correctly authenticated when the MIT agreement was set up. (i.e. the fact that the payment is made with a stored credential does not make it out of scope). Note that if the credential is only held until the end of the stay or rental, this is not considered a stored credential.

3.1.2 Exceptions to requirement to authenticate.

Authentication is not required at the time of booking only if:

1. No payment is to be taken prior to the customer being able to authenticate through a face to face transaction at the time of check-in/delivery of the service. This will be the case if:
    - No payment is due at time of booking, and
    - There is no requirement for either the booking agent or the T&H supplier to collect any payment from the customer through an MIT before the customer is able to authenticate through a face to face authenticated transaction at check in (or via a CNP transaction in case of an express/keyless/non face to face check in) or another subsequent CIT, for example when there is no guaranteed reservation.
2. The booking transaction is out of scope of SCA, specifically:
    - The booking transaction is a MOTO transaction

- The booking transaction is one-leg out, i.e. the card is issued or the transaction is acquired outside of the EEA or UK, however note that in this case best efforts should be applied to apply SCA
- The booking is made using an anonymous payment instrument, for example an anonymous prepaid card.

Merchants and Acquirers need to ensure that out of scope transactions are correctly identified and indicated as such, otherwise the lack of authentication can lead to declines. They must also ensure that transactions are not mis-classified as out of scope. Intermediaries who are passing booking and authentication information between booking agents and suppliers or are processing payments on behalf of suppliers will need to ensure they can receive and pass the required information/indicators for Out of Scope transactions. For more information see Appendix A.3.

For more information on the definition, flagging and identification of out of scope transactions and for the use of exemptions, please refer to *PSD2 SCA for Remote Electronic Transactions Implementation Guide*.)

3.1.3 The EMV 3DS Travel Industry Message extension

The EMV Travel Industry Message extension is for travel & hospitality merchants to provide travel-related data to ACSs for their use in risk-decisioning in EMV 3DS 2.1 and above. For example, airlines can provide data related to the travel itinerary such as departure and arrival location, number of passengers on the ticket etc. and hotel and car rental merchants can provide data related to the reservation such as duration/location of stay/rental.

Visa support this EMVCo extension so the data can optionally be sent by merchants in the EMV 3DS authentication request message, but there is limited information at this time whether Issuers/their ACS use this data in 3DS decisioning.

3.2 Principle 2: An authorization request must take place within 72 hours of booking, with proof of authentication (or be marked out of scope)

A CIT must take place at the time of booking to:

- Collect funds due at booking and/or
- Set up a “Merchant Initiated Transactions” (MIT) agreement for funds to be collected later

When no payment is due at booking but an MIT must be set up, this CIT must be completed as an account verification transaction with zero value.

When the transaction is setting up an MIT, the transaction ID of this initial CIT must be stored and populated within authorization request(s) for the subsequent MIT(s).

3.2.1 Authentication data requirements in the authorization request

The authorization request associated with this CIT must either contain the authentication data or be correctly flagged as out of scope or exempted from SCA. For more information on the required data, please refer to the *PSD2 SCA for Remote Electronic Transactions Implementation Guide*.

In the case of an indirect booking where the booking agent requests authentication but the funds are to be collected by the T&H supplier[6], the authorization request must be submitted by the T&H supplier as the merchant (or its processor/GDS). The merchant must receive this authentication data and process an authorization within 72 hours of the booking authentication.

This authorization request/account verification, even if only performed to set up an MIT agreement, cannot be completed by the booking agent: it must be completed by the merchant. This means that the systems used by the booking agent and merchant must be upgraded to allow the booking agent to pass the authentication data or an exemption/out of scope indicator to the merchant.

There is one exception to this: the authorization request/account verification performed to set up an MIT agreement can be completed by the booking agent if the booking agent is the corporate head office of the brand under which the supplier/merchant is operating as a branded franchisee. In this case, the booking agent, could perform the authorization request (CIT) to set up the MIT and pass the Tran id for the merchant to process subsequent MITs instead of passing the authentication data.[7]

Where systems are currently unable to pass this data, an interim solution may be used to flag these transactions to Issuers so they are less likely to be declined due to lack of authentication data. This solution which is described in section 4.6 is available for a limited period to allow stakeholders to make necessary systems upgrades. It can only be used for indirect booking transactions.

3.2.2 No more manual key entry

Transactions originating as ecommerce bookings can no longer be manually entered into a POS terminal by a merchant or intermediary or be processed as a "MOTO" transaction. Such manually processed transactions may be declined due to lack of proof of authentication. Transactions may only be initiated and processed as MOTO for bookings made by telephone.

This means that to process all transactions which originate from ecommerce bookings, merchants must move to integrated payment solutions enabling them to include the required authentication data with all authorization requests for all CIT transactions associated with or direct or indirect bookings. Furthermore, merchants cannot initiate an MIT through manual key entry without the MIT having been set up via a CIT containing authentication data.

The only exception to this is if the interim solution for transactions resulting from indirect bookings described in section 4.6 is being deployed and the strict conditions governing the application of the interim solution are adhered to.

[6] For other potential models, refer to section 4

[7] The Booking Agent can only do this on behalf of the supplier when it can use the same brand name in the CIT as the one that will be used in the MIT by the supplier. If the agent is not using the same brand name, then the CIT to set up the MIT can only be completed by the supplier.

3.3 Principle 3: authentication and authorization amount must be for the amount due at booking.

If a payment is due at booking, then the amount authenticated and authorized must the amount due at the time of booking.

If no payment is due at the time of booking but SCA is required, for example to set up an agreement to collect a no show fee as an MIT as part of the supplier's cancelation policy, the amount authenticated and authorized must be zero, i.e. an account verification transaction is processed.

- When authenticating a zero value transaction the "PA" message category must be used in EMV 3DS rather than the NPA category[8]
- When authenticating for an MIT set up agreement, an SCA challenge must be requested via EMV 3DS. No exemption may be applied, unless the transaction qualifies for the SCP exemption

If a booking made through a booking agent is to be fulfilled by multiple T&H suppliers acting as merchants and the authentication is requested by the booking agent, the amount authenticated must follow the same principle, i.e. it must be the total due at time of booking across all of the merchants.

Examples:

1. No deposit or payment is due prior to check in, but the merchant needs to set up an agreement to collect a cancellation fee of €80 as an MIT in the case of a "no show":
    - Present the terms and conditions governing the cancellation policy and the collection and amount of the MIT no show fee and request authentication and authorization for a zero amount
    - In case of a No show, the cancelation fee is collected via an authorization request as an MIT for €80
2. No payment is due at booking but prepayment of €500 is to be collected as an MIT prior to check-in:
    - Present the terms and conditions governing the prepayment MIT, including when the repayment will be collected, and the amount that will be charged and request authentication and authorization for a zero amount
    - When the €500 is due, it is collected via an authorization request as an MIT for €500
3. A €1000 deposit is due on booking and a €500 balance payment is due two weeks prior to check-in:
    - Present the terms and conditions governing the deposit and balance MIT, including when the balance payment will be collected, and the amount that will be charged and request authentication and authorization for €1,000
    - When the €500 is due, it is collected via an authorization request as an MIT for €500

[8] Please refer to the EMVCo 3DS specification for more information on message categories

4. No deposit or payment is due prior to check in, but the merchant needs to set up an agreement to either collect a cancellation fee of €80 as an MIT in the case of a "no show" or to collect all fees at the end of the stay (and possibly beyond the stay in the case of delayed charges such as mini bar charges)
    - Present the terms and conditions governing the cancellation policy and of the collection of the MIT no show fee and the terms and conditions governing the calculation of the full stay (e.g. €120 per night plus any additional charges) and request authentication and authorization for a zero amount
    - When the customer check-in "not in person" (express check-in), an authorization request is sent for the pre-agreed 3-night stay as an MIT Reauthorization for €360

3.4 Principle 4: Any payment initiated by a merchant after booking or after check-in when the cardholder is unavailable to authenticate must be processed as an MIT

As stated in section 2.5.1, MITs are out of scope of SCA and do not require authentication at the time the payment is collected, so long as terms and conditions are presented to the customer and authentication is performed when the MIT agreement is set up. This applies to:

- Payments taken by an agent on behalf of a T&H supplier, or by the T&H supplier after booking but before check-in. These must be authenticated at booking, and all applicable terms and conditions that govern the collection of the MITs must be presented before authentication, including when the authentication is requested by the booking agent
- Payments taken by the T&H supplier after check-in where the T&H supplier may request authentication either:
    - Through a face to face transaction at check-in using Chip & PIN, or other appropriate cardholder verification method in the case of mobile payments, or
    - Through EMV 3DS in the case of an "express" or "keyless" check-in facilitated through the T&H supplier(s) website or mobile app

3.4.1 MITs must be governed by a customer agreement set up through an authenticated transaction

For MITs to be processed as out of scope (without SCA), Terms and Conditions (T&Cs) of the MIT agreement for all payments to be taken without the cardholder being available to initiate or authenticate must be clearly presented to the cardholder by:

- The party undertaking authentication at the time of booking[9], where:
    - MITs are to be taken before check-in, and/or no show fees may apply, and

[9] In the case of a direct booking where the T&H supplier is authenticating and acting as the merchant, this will be the T&H supplier. In the case of an indirect booking, where the booking agent is authenticating, the terms and conditions will be presented by and the SCA challenge will be requested by the booking agent on behalf of the T&H supplier/merchant

  - There will not be an opportunity to apply SCA through another face to face or CNP authentication directly with the merchant to cover all fees after check in; or

- The supplier/merchant at time of check-in or check-out if MITs may be used to collect incremental charges after check-in or delayed charges after check-out

T&H suppliers/merchants that collect funds and that wish their booking agents to request authentication at booking must update contractual agreements with their agents to request that they request authentication and disclose the MIT agreement Terms and conditions to customers. If terms and conditions for potential future MITs, for example for incremental charges incurred during the course of a stay, cannot be presented by the booking agent at booking, the merchant must present these terms and conditions and request authentication at check-in, through either a face to face or CNP transaction as described above.

3.4.2 MITs must be correctly identified using the Visa MIT Framework and the Tran ID must be provided

Subsequent transactions that are to be processed as MITs must be correctly indicated using the MIT Framework which entails:

- Identifying the MIT type (i.e. the transaction purpose) and
- Populating the Tran ID of the initially authenticated or previous transaction.

This means that merchant payment systems must be capable of storing the Tran ID from the original CIT, so that it can be populated in any subsequent MIT. Note some Acquirers and gateways may be able to store this Tran ID on the merchant's behalf. Alternatively, it may be stored in the reservation system, depending on the merchant set up, and so long as the reservation and payment systems are integrated.

Refer to the PSD2 SCA for Remote Electronic Transactions Implementation Guide for more details on the Visa MIT Framework. Merchants/processors must check how they should indicate MITs to their gateway or Acquirer as this may differ between different gateways and Acquirers.

3.4.3 MITs set up and authenticated through a transaction that takes place at check in

Delayed or incremental charges, such as for mini-bar use or refueling a rental car, that have been authenticated and pre-authorized through a face to face transaction or CNP transaction during check-in or check out and that will be collected when the customer is not available to initiate or authenticate the transaction must be processed as MITs. These transactions must be correctly indicated to prevent risk of declines.

In order to process these transactions as MITs, the merchant's POS system must be upgraded to ensure the authorization request contains the required data elements to indicate an MIT as detailed in section 3.4.2.

In order to apply SCA as required when setting up the customer agreement to take these MIT payments, either Chip and PIN, or other cardholder verification method in the case of a mobile transaction, or EMV 3DS in the case of a CNP transaction is required.

3.5 Principle 5: Booking agents and merchants have options for requesting authentication for an indirect booking,

Several options exist for T&H suppliers and booking agents to ensure authentication is performed and transactions are processed as required. Approaches include but are not limited to the options summarized in Table 3. Merchants and booking agents must mutually agree which to adopt. If merchants and booking agents consider alternative options to these, they should speak to their Acquirer and or gateway to ensure that the option can be supported.

Table 3: Summary of Options and Considerations

Option	Description	Considerations
Option 1 T&H Supplier requests authentication & acts as merchant	The booking agent either: • Sends the customer a link to the supplier's own website payment page • Sends booking details without any payment information to the T&H supplier, who then contacts the customer via email or SMS with a link to its own website payment page The T&H supplier then handles authentication & payment collection as the merchant	• The whole transaction is processed as a direct sale by the T&H supplier and may not require booking system upgrade
Option 2 Booking agent requests authentication & acts as merchant	The booking agent requests authentication at booking and collects <u>all</u> required payments on the T&H supplier's behalf at the time of payment agreed upon with the cardholder. The Booking Agent subsequently pays the T&H supplier(s) through a separate B2B transaction(s)	• Does not require booking system upgrade at the T&H supplier • Allows the booking agent to collect agreed prepayments and no show fees • Where these payments are collected subsequent to booking, they must be processed as an MIT as described in principle 4 • The T&H supplier may subsequently collect additional payments but only if it performs a further authentication through a face to face or CNP transaction at check-in or check-out • May require renegotiation of booking agent/supplier agreements • May require setting up of a payment process between the booking agent and T&H supplier e.g. virtual card • May impact T&H supplier cash flow
Option 3 Booking agent requests authentication,	The booking agent requests authentication at booking and sends authentication and associated payment data to the	• Maintains current user experience and business models under which the T&H supplier collects payment

T&H supplier acts as merchant	supplier to request its own authorization to collect payment as the merchant	• Requires the T&H supplier and intermediaries to upgrade and integrate systems to pass additional data • Payments collected by the T&H supplier after the time of booking are MITs and must be correctly set up and authenticated through a CIT at booking and then correctly indicated as MITs by suppliers/Acquirers to avoid declines.
Option 4 Booking agent requests authentication, and both parties act as merchant in turn	The booking agent requests authentication at booking and sends authentication and associated payment data to the supplier. Both parties request authorization to collect their respective payments as required	• As option 3, except that, in addition for some payments to be collected by the supplier later as MITs, some payments are also collected by the booking agent (as a CIT at booking or subsequently as MIT(s))

Not all of the above options may be possible or appropriate for all agents and T&H supplier. Suppliers should consider the impacts to customers and business models when planning for SCA compliance. The first two options enable suppliers to avoid upgrading to integrated payment solutions that allow the passing of authentication data from the booking agent but may cause disruptions to the supplier's customers or business model.

The options and the considerations that apply to each party are described in more detail in section 4.

3.6 Principle 6: Corporate T&H payments may qualify for the secure corporate payments (SCP) exemption

If a booking is made for corporate purposes and is initiated electronically through a secure, dedicated payment process or protocol that is not available to consumers and uses an eligible commercial card, the transaction may, subject to the view of local regulators, be eligible for the Issuer to apply the SCP exemption. Please refer to the *PSD2 SCA Secure Corporate Exemption Guide* for more information.

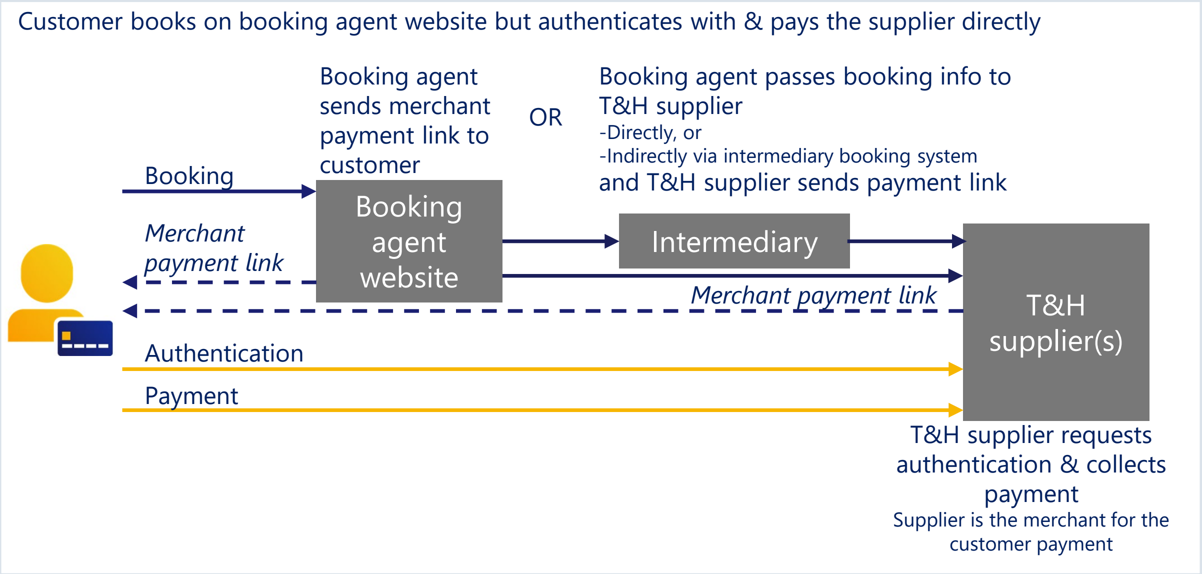
4. Indirect booking

As summarised in principle 5 in section 3.5 above, T&H suppliers and booking agents have options for the authentication and processing of payments for indirect bookings.

4.1 Option 1: T&H supplier requests authentication & acts as merchant

Under Option 1, where the supplier acts as merchant and requests authentication[10],[11]and collects payment, the process for the supplier is the same as it would be for a direct booking.

Figure 3: Option 1 T&H Supplier requests authentication & acts as merchant


Customer books on booking agent website but authenticates with & pays the supplier directly
Booking agent sends merchant payment link to customer
OR
Booking agent passes booking info to T&H supplier
-Directly, or
-Indirectly via intermediary booking system
and T&H supplier sends payment link
Booking
Merchant payment link
Booking agent website
Intermediary
Merchant payment link
T&H supplier(s)
Authentication
Payment
T&H supplier requests authentication & collects payment
Supplier is the merchant for the customer payment

With this option, the T&H supplier can collect any payments covered by the T&Cs displayed before authentication. Refer to section 3.4.1 for more details. For any payment conditions not covered at that time, another authentication will be required at check-in (F2F or CNP) before any further payment can be taken.

Some intermediaries may offer solutions that generate the T&H supplier link that can be sent to the customer to enable them to authenticate and pay.

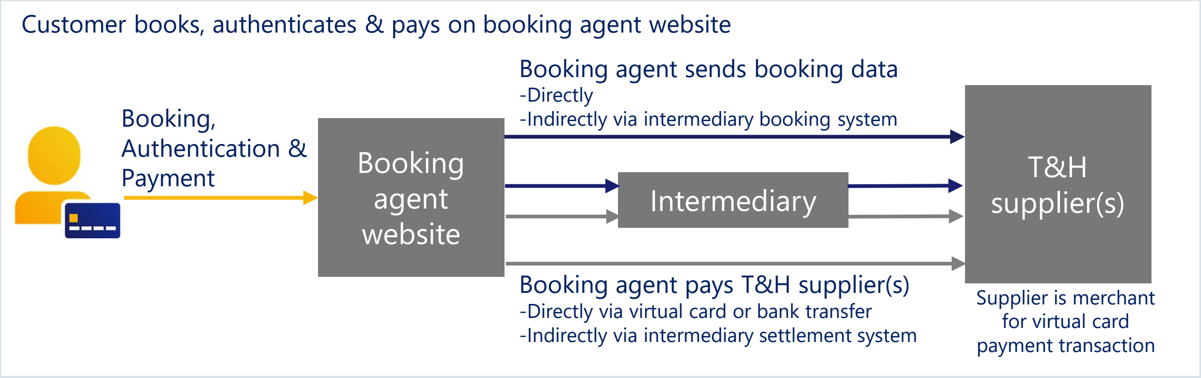
4.2 Option 2 - The booking agent requests authentication and is the merchant:

The booking agent collects all required payments on the supplier's behalf at the time of payment agreed upon with the cardholder (e.g., at booking, at a specified time preceding check-in, or at a pre-agreed date in the case of a cancellation / no-show fee).

[10] Unless the transaction, is out of scope or qualifies for an exemption.

[11] In the case of airlines, the GDS could potentially handle this on behalf of the supplier.

Figure 4: Option 2 Booking agent requests authentication & acts as merchant


Customer books, authenticates & pays on booking agent website
Booking, Authentication & Payment
Booking agent website
Booking agent sends booking data
-Directly
-Indirectly via intermediary booking system
Intermediary
T&H supplier(s)
Booking agent pays T&H supplier(s)
-Directly via virtual card or bank transfer
-Indirectly via intermediary settlement system
Supplier is merchant for virtual card payment transaction

Under this model, the booking agent:

- Is acting as the merchant collecting the funds for this/these end customer transactions
- Requests authentication for the customer card transaction for the total amount due at booking, as described in sections 3.1 and 3.3.[12,13]
- Submits the transaction(s) made with the customer card to authorization as indicated in section 3.2 and 3.3, and 3.4 in the case of MITs, and 3.6 if the SCP exemption applies:
    - A transaction at booking is authenticated and authorized as a CIT
- A payment collected by the booking agent after booking or at check-in when the customer is not available to authenticate, can be processed as an MIT, so long as an authenticated agreement is in place to collect those payments as indicated in section 3.4[14].
- Subsequently pays the T&H supplier(s) via a B2B transaction(s) typically using a commercial virtual card issued to the booking agent, Visa Direct, bank transfer or intermediary settlement system.

With this option, no further payment can be collected by the T&H supplier(s) until another authentication (F2F or CNP)can be performed (i.e., at check-in or checkout[14]).

[12] Unless the transaction is out of scope or an exemption may apply

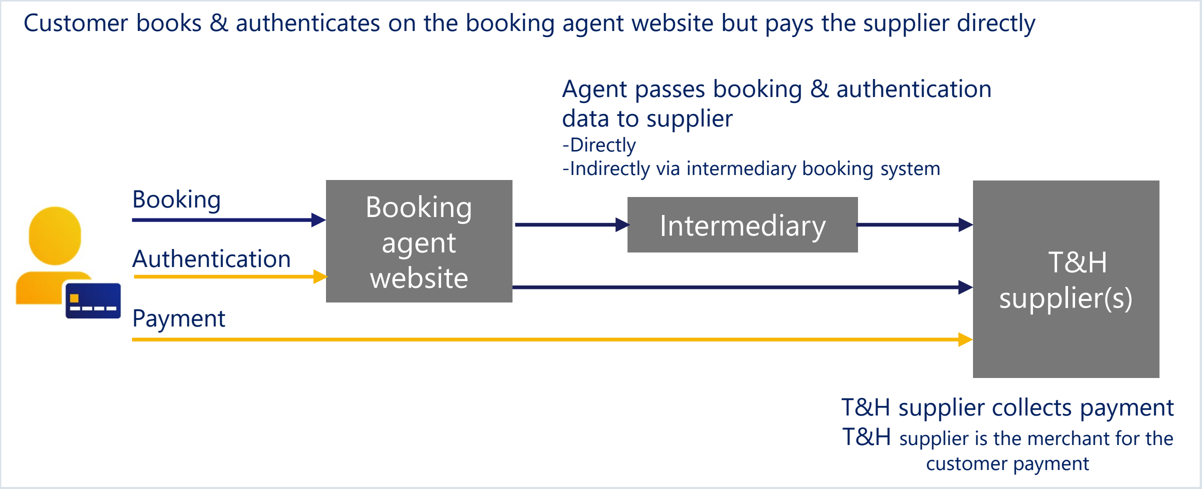
[13] Authentication could also be requested if T&Cs are being agreed in order to allow collection of other/ final payment through MIT(s) at check-in and/or at/after check-out

[14] It is customary that the Booking Agent only collects a set fee for the stay or a no show fee and that any additional charges are collected by the T&H supplier later at/after check-out. For this the T&H supplier will need to set up and request SCA for a separate MIT agreement at check-in or check-out. It would be possible, if the T&H supplier so desire/agrees with its Booking Agent, that the Booking Agent collects other fees after check-in/check-out, provided full T&Cs can be displayed by the Booking Agent to the cardholder at time of booking/authentication.

4.3 Option 3 The booking agent requests authentication and the T&H supplier is the merchant

Under this option, the booking agent requests authentication and the T&H supplier(s) is(are) responsible for collecting all required payments.

Figure 5: Option 3 Booking agent requests authentication & T&H supplier acts as merchant


Customer books & authenticates on the booking agent website but pays the supplier directly
Agent passes booking & authentication data to supplier
-Directly
-Indirectly via intermediary booking system
Booking
Authentication
Payment
Booking agent website
Intermediary
T&H supplier(s)
T&H supplier collects payment
T&H supplier is the merchant for the customer payment

The booking agent:

- Requests authentication[15] on the card for the amount due at booking and/or to set up any MIT agreement required for the T&H supplier(s)[16], as described in sections 3.1 and 3.3, to take one or several subsequent payment(s) when the customer is not available to initiate or authenticate the payment
- Passes the authentication and associated payment data to the T&H supplier(s)[17] [18]

The T&H supplier(s)[17]:

- Receive(s) the booking details including the authentication and associated payment data[19]

[15] Unless the transaction is out of scope or qualifies for an exemption.

[16] For details of how a booking agent requests authentication on behalf of multiple merchants please refer to section 5.2

[17] Or, for airlines, to the GDS processing the transaction on behalf of the supplier where applicable.

[18] For detail on which data is to be passed refer to Appendix A.3

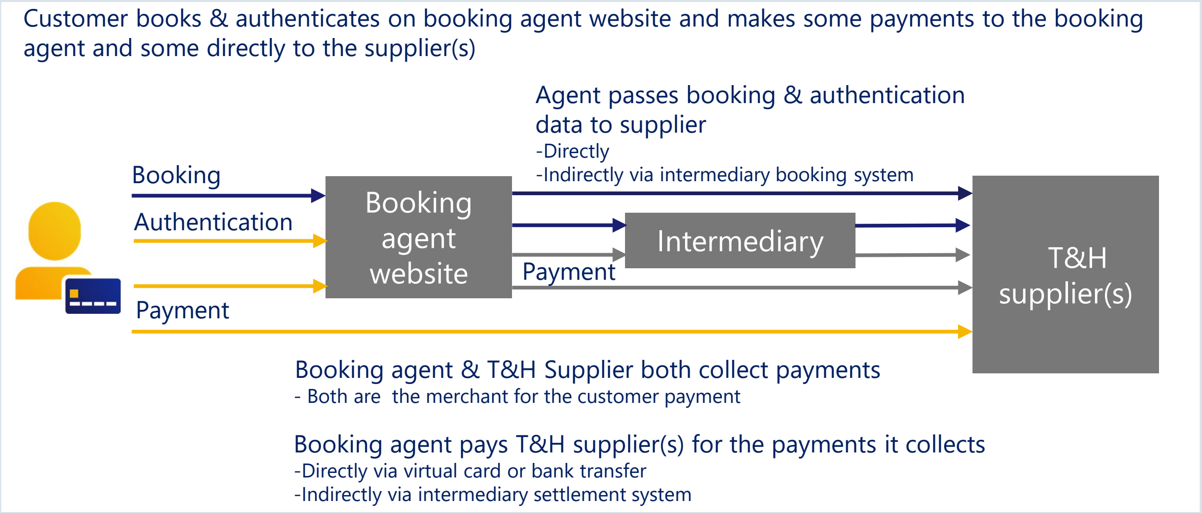
[19] Or the Tran ID in the case that the booking agent is the corporate head office a branded franchisee supplier group and it performed this initial authorization request to set up the MIT using the same brand name.

- Submit(s) an authorization request(s) at time of booking as described in section 3.2 and 3.3, and 3.4 in the case of MITs, and 3.6 if the SCP exemption applies[20]:
    - For the amount it is (they are) collecting as the merchant and/or
    - To set up the MIT mandate via a CIT for any payment due later
- Subsequently submit(s) an authorization request(s) as an MIT (including indicating the MIT type as described in section 2.5.1and 3.4) for any payment due after booking and covered by the T&Cs.
- For any further payment not covered by the T&Cs agreed at booking, the merchant must ensure an SCA is requested at check-in (either F2F or CNP)

4.4 Option 4: The booking agent collects partial payment and the T&H supplier collects remaining payments

This option allows the booking agent to collect partial payment on the T&H supplier's behalf, and the T&H supplier(s) to subsequently collect additional payments. For example a booking agent may collect a deposit or partial prepayment at time of booking or at a later time agreed with the cardholder and the T&H supplier(s) may collect the balance prior to check in, a no show fee, or a final payment/delayed charges in case of a card not present express check-in/check-out).

Figure 6: Option 4 Booking agent requests authentication & booking agent & T&H supplier both act as merchants


Customer books & authenticates on booking agent website and makes some payments to the booking agent and some directly to the supplier(s)
Agent passes booking & authentication data to supplier
-Directly
-Indirectly via intermediary booking system
Booking
Authentication
Payment
Booking agent website
Intermediary
Payment
T&H supplier(s)
Booking agent & T&H Supplier both collect payments
- Both are the merchant for the customer payment
Booking agent pays T&H supplier(s) for the payments it collects
-Directly via virtual card or bank transfer
-Indirectly via intermediary settlement system

Under this option:

The booking agent:

- Requests SCA[21] on the customer card for the amount due at booking and to set up any MIT mandate required for either or both the booking agent and/or the T&H supplier to take a subsequent payment as appropriate

[20] Unless this authorization (CIT) has already been performed by the corporate head office of a branded franchisee supplier group, in which case this step is skipped.

[21] Unless the transaction is out of scope or an exemption may apply.

- Submits a CIT authorization request at time of booking as indicated in section 3.2 and 3.3:
    - For the amount it is collecting as the merchants and/or
    - To set up an MIT mandate for the booking agent is to collect any fees later
- Passes the authentication and associated payment data to the T&H supplier[22,23]
- Subsequent payments collected by the booking agent when the customer is not available to initiate or authenticate the transaction can be processed as MITs as in section 3.4.
- When required/agreed with the T&H supplier, the booking agent pays the T&H supplier(s) via a B2B transaction, typically using a commercial virtual card, Visa Direct, a bank transfer or intermediary settlement system.

The T&H supplier(s)[24]:

- Receive the booking details including the authentication and associated payment data
- Submits a CIT authorization request within 72 hours of booking as indicated in section 3.2 to set up an MIT mandate as indicated in section 3.4.2[25]
- For any payment(s) where the T&H supplier is responsible to collect funds due later than booking, they can be processed as MITs.
- Subsequent payments collected by the T&H supplier(s) when the customer is not available to initiate or authenticate the transaction can be processed as MITs according to the T&Cs agreed with customer

4.5 Additional considerations for indirect bookings

The following additional considerations need to be taken into account for indirect bookings:

4.5.1 Selection of the options

Not all options above may be possible or appropriate for all T&H suppliers. Suppliers should consider the impacts to customers and business models when planning for SCA compliance.

[22] Or, for airlines, to the GDS processing the transaction on behalf of the supplier, where applicable.

[23] For detail on which data to be passed refer to Appendix A.3

[24] Or, for airlines, the GDS processing the transaction on behalf of the supplier, where applicable

[25] When the booking agent and T&H supplier are both collecting funds, each entity must process its own separate authorization request within 72 hours of booking, to set up its own MIT agreement and obtain its own Tran ID that it will then submit with the subsequent MITs it collects. For Visa transactions, the only exception is if the Booking Agent is the corporate head office of the brand under which the supplier/merchant is operating as a branded franchisee, as described in section 3.2.1. In this case, the booking agent may process a single authorization request to set up an MIT agreement that applies to both parties and the resulting Tran ID may be passed to the supplier and may be submitted by both parties alongside subsequent MIT authorization requests as long as the brand name used by the head office and the franchisee are the same.

As highlighted in the considerations column of Table 3, Options 1 & 2 enable suppliers to avoid upgrading to integrated payment solutions but may cause disruptions to customers and/or business models.

Option 3 enables the T&H supplier to continue collecting payments without needing to re-contact the customer for authentication (as in option 1), or relying on the booking agent to make a timely supplier payment, but requires the use of an integrated payment solution across all parties in the booking chain to receive and send the required data.

Under all options, payments taken after the time of booking are MITs and in principle out of scope of SCA, as long as an agreement for the collecting party to charge the cardholder was made and authenticated at the time of booking and the cardholder is not available to initiate or authenticate the transaction at the time the payment is collected. Under options 3 & 4, authentication must be requested by the booking agent on behalf of the T&H supplier, and the transactions must be appropriately handled and flagged in accordance with section 3.4.

4.5.2 Intermediaries in the booking and transaction processing chain & integration of systems

In many cases bookings taken by booking agents are managed through intermediaries and third-party systems including GDSs, aggregators and hotel brand PMSs. Intermediary systems may not yet be integrated into booking agent and T&H supplier systems in a way that allows authentication data to be passed to merchants with the following consequences for options 3 and 4 above:

- It may be difficult for a T&H supplier to identify the source of the original customer booking
- The legacy booking process of the T&H supplier may include manual intervention, for example hotel/car rental reception staff reading booking information from a PMS/CRS and manually initiating the payment transaction. As stated in section 3.2.2, transactions originating from an ecommerce booking can no longer be manually entered into a POS terminal by a merchant or intermediary or be processed as a "MOTO" transaction.

Booking agents, intermediaries and T&H suppliers need to ensure that systems are integrated to allow the automatic passing of authentication and transaction data as defined in Appendix A.3. However, until all systems can be upgraded to enable a T&H supplier using option 3 and/or 4 to obtain the required authentication data to process its transactions, an interim solution described in section 4.6 can be used.

Guidance for booking agents, Issuers and GDSs on determining one-leg-out status and ensuring SCA can be applied to transactions that are in scope. One-leg-out transactions can be identified by Issuer BINs and Acquiring Institution Country Codes in Authorization requests and an Acquirer Country Code (ACC) extension in EMV 3DS. It is important to note that it is the Acquirer location, not the merchant location that determines whether a transaction is one-leg-out or in scope of SCA.

Booking agents must take this into account when they handle authentication for a merchant that will process its own EEA / UK acquired authorization which will be in scope of SCA. To ensure SCA is applied when it will be required by the merchant's acquiring BIN, booking agents should either:

- Always request a challenge in the EMV 3DS authentication request (AReq)26 when the acquiring BIN used by the agent in the authentication request is not from an EEA / UK Acquirer and/or
- Use an EEA / UK acquiring ID in the AReq, with appropriate permission, so that the Issuer identifies the transaction as in scope of SCA.

All parties should remember even when transactions are one leg out, 'best efforts' to apply SCA should be made. In Visa's view the following use cases and interpretations may apply:

1. A transaction uses a card issued in the EEA or the UK, but is acquired outside the EEA or the UK: in this case the Issuer should decide whether to approve, challenge (where possible) or decline the transaction based on their risk assessment, the liability implications and the impact on the consumer experience.
2. A transaction uses a card issued outside the EEA or the UK, but is acquired within the EEA or the UK: in this case, we would recommend that Acquirers/merchants send transactions in an SCA compliant way, such as via EMV 3DS, where the Issuer supports this. The Issuer is not obliged to apply SCA.

For more details please refer to the PSD2 *SCA for Remote Electronic Transactions Implementation Guide* sections 2.3.2 and 2.3.3.

4.5.3 Use of commercial virtual cards for payment of a T&H supplier by a booking agent

In options 2 and 4 where a booking agent has collected payment from the customer on behalf of the T&H supplier, the booking agent may use a commercial virtual card to subsequently pay the T&H supplier. In this case, the SCP exemption may apply, and the Issuer needs to ensure that it identifies the transaction as such and does not apply or request SCA or decline because SCA has not been applied. For more information please refer to the *PSD2 SCA Secure Corporate Payments Exemption Implementation Guide*.

4.6 Interim solution for transactions resulting from indirect booking

To avoid declines of transactions resulting from indirect bookings until systems are upgraded when options 3 and 4 described in sections 4.3 and 4.4 are selected, and a merchant is able to receive proof of authentication to include in its transactions, a merchant can, on an interim basis, omit submitting a CIT authorization request with proof of authentication to set up the MIT and can directly submit the MIT transaction when payment is due. As these transactions will not have the required information to be correctly indicated as MITs, they can, on an interim basis, be indicated as out of scope using the MOTO (Mail Order / Telephone Order) indicator. This indicator is already recognized by Issuers and used to handle out-of-scope transactions.

In the Visa authorization system, the MOTO indicator is a value of 08 in Field 25, and/or Value of 01 or 04 in Field 60.8.

[26] Request for an SCA challenge to be applied is only supported in EMV 3DS version 2.1 or higher

4.6.1 Conditions for use of the MOTO indicator as an interim solution

The option to use the MOTO indicator to flag MITs will exist on an interim basis only, and is limited to certain merchant category codes (MCCs) as listed in Appendix A.2, and to transactions originating from indirect sales where authentication has been requested by the booking agent or where the SCP exemption may apply. The conditions summarised in Table 4 apply to the use of the MOTO indicator in travel and hospitality MITs resulting from indirect sales. A merchant must discuss this with its Acquirer to determine eligibility.

Table 4: Conditions for use of the MOTO indicator as a temporary solution for flagging MITs for indirect Travel and Hospitality transactions

Stakeholder	Requirements (from SCA enforcement Date, for all in-scope transactions)
Booking Agents	Agents taking bookings must: • Clearly present the terms and conditions of the MIT agreement to the customer at the time of booking and before authentication.[27] • Request SCA for the booking as an MIT agreement, unless the SCP exemption can be used as agreed with the merchant's Acquirer (no other exemption can be used when setting up an MIT). Note: These obligations also apply to anyone handling direct sales when they will need to process MITs.
Merchants	Eligible merchants must have updated contractual agreements with their customer-facing third party agents taking bookings on their behalf (and with any third party provider involved in the bookings) to confirm the above requirements for booking agents are in place. In cases where SCA was performed but the merchant does not have proof of authentication of the MIT agreement, MITs resulting from indirect sales may temporarily be presented for authorization with the MOTO indicator[28] until the chain of intermediaries is updated. The MOTO indicator can only be used when the transaction is either: • A legitimate MOTO transaction, or • An SCA-compliant MIT where SCA took place to set up the MIT but where proof of authentication at setup is not yet available due to the transaction being associated with an indirect sale.[28]
Acquirers	Acquirers are responsible for ensuring that all transactions sent to Issuers with the MOTO indicator have been completed in an SCA-compliant manner. Acquirers must put in place: • Contractual obligations with their travel and hospitality merchants that are permitted to use the MOTO indicator, confirming the above requirements for merchants have been met • Controls to monitor compliance with these measures

[27] Refer to the Visa Rules for specific required terms and conditions for MITs according to transaction type (for example, for guaranteed reservations).

[28] The use of the MOTO indicator for this purpose can only be used by merchants from the MCCs listed in Appendix A.2

Visa has updated its PSD2 supplemental rules to include the above SCA obligations and will be monitoring usage and fraud rates on any transactions submitted with the MOTO indicator to ensure the indicator is not abused or resulting in any increased fraud. Improper usage will be subject to removal of the right to use the indicator.

4.6.2 Issuer Impacts

Visa estimates that the MOTO indicator has historically been used for a significant proportion of Travel and Hospitality indirect sales transactions where primary account numbers (PANs) are manually key entered into POS systems by merchants. Use of the interim solution will result in the MOTO indicator being applied for a portion of the remaining key-entered, transactions that have not historically been flagged as MOTO, so the number of MOTO transactions from the Travel and Hospitality sector is expected to increase.

Issuers should not systematically decline MOTO transactions that are sent without proof of authentication from T&H merchants, however Issuers should continue to perform risk-based authentication (RBA) on any MOTO transactions before making an authorization decision.

It is possible that some of the transactions currently key-entered without any MOTO indicator may not be upgraded to include the MOTO indicator in time for the regulatory enforcement date. These transactions may appear to be in-scope and presented without SCA. Issuers will need to consider which authorization decision to take in those circumstances.

For additional considerations on merchant interim usage of the MOTO Indicator and Issuer and Acquirer impacts please refer to *Visa Business News: Preparing Travel and Hospitality Merchants for SCA Compliance on Indirect Sales Transactions 20 August 2020* and *PSD2 Strong Customer Authentication for Remote Electronic Commerce Transactions – European Economic Area: Visa Supplemental Requirements*.

4.7 The long-term solution is to process transactions as MITs through integrated systems

The long-term solution to managing indirect booking transactions when business model options 3 and 4 (refer to section 3.5) are selected, is described in that section.

Merchants are reminded that the use of the MOTO indicator to flag MITs resulting from indirect sales is only a temporary solution and they must work toward longer-term solutions based on integrated booking systems across the indirect booking chain.

Industry-level technical guidance on which data elements must be passed from booking agents to suppliers is included in Appendix A.3. This guidance will assist stakeholders in upgrading systems to pass this data.

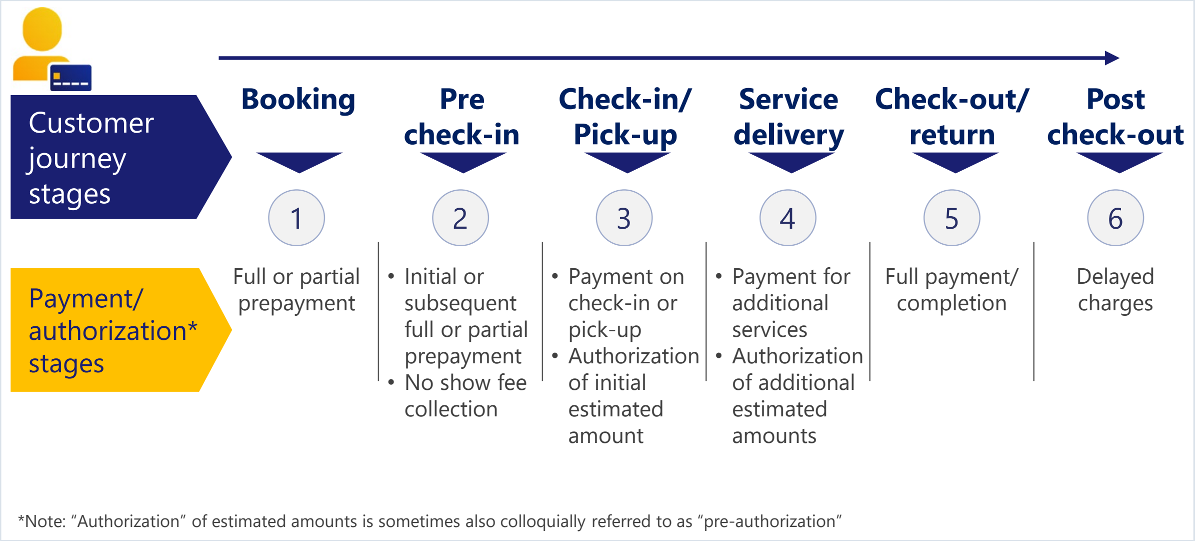
5. Authentication & authorization process flows

This section summarises the key steps in the authentication flow when the authentication is requested by the booking agent.

It then summarises the key steps in the authorization flow for the following payment types

- A prepayment – at time of booking, or later (but prior to check in) – Stages 1 & 2 in Figure 7
- A "no show" payment – Stage 2 in Figure 7
- Payments from check in to check out – Stages 3 to 5 in Figure 7
- Payments for delayed charges – Stage 6 in Figure 7

Figure 7: Customer journey stages and payment types



Customer journey stages
Payment/ authorization* stages
Booking
Pre check-in
Check-in/ Pick-up
Service delivery
Check-out/ return
Post check-out
1
2
3
4
5
6
Full or partial prepayment
• Initial or subsequent full or partial prepayment
• No show fee collection
• Payment on check-in or pick-up
• Authorization of initial estimated amount
• Payment for additional services
• Authorization of additional estimated amounts
Full payment/ completion
Delayed charges

*Note: "Authorization" of estimated amounts is sometimes also colloquially referred to as "pre-authorization"

For each of the four above payment types, the detailed steps to follow are presented for three different use cases, i.e. for when the booking is:

- Direct with the merchant (see section 5.3.1)
- Indirect via the booking agent who handles authentication only (see section 5.3.2) and
- Indirect via a booking agent who handles the authentication and the payment (see section 5.3.3)

5.1 Authentication flow

In direct booking scenarios and the indirect booking scenario options where:

- The T&H supplier requests authentication and acts as the merchant (option 1 as described in section 4.1), or
- The booking agent requests authentication and acts as the merchant (option 2 as described in section 4.2)

and where the transaction is in scope of SCA and requires authentication at time of booking, the merchant requests authentication through EMV 3DS, and then submits the CIT authorization request with the authentication data as it would for a normal remote electronic transaction[29].

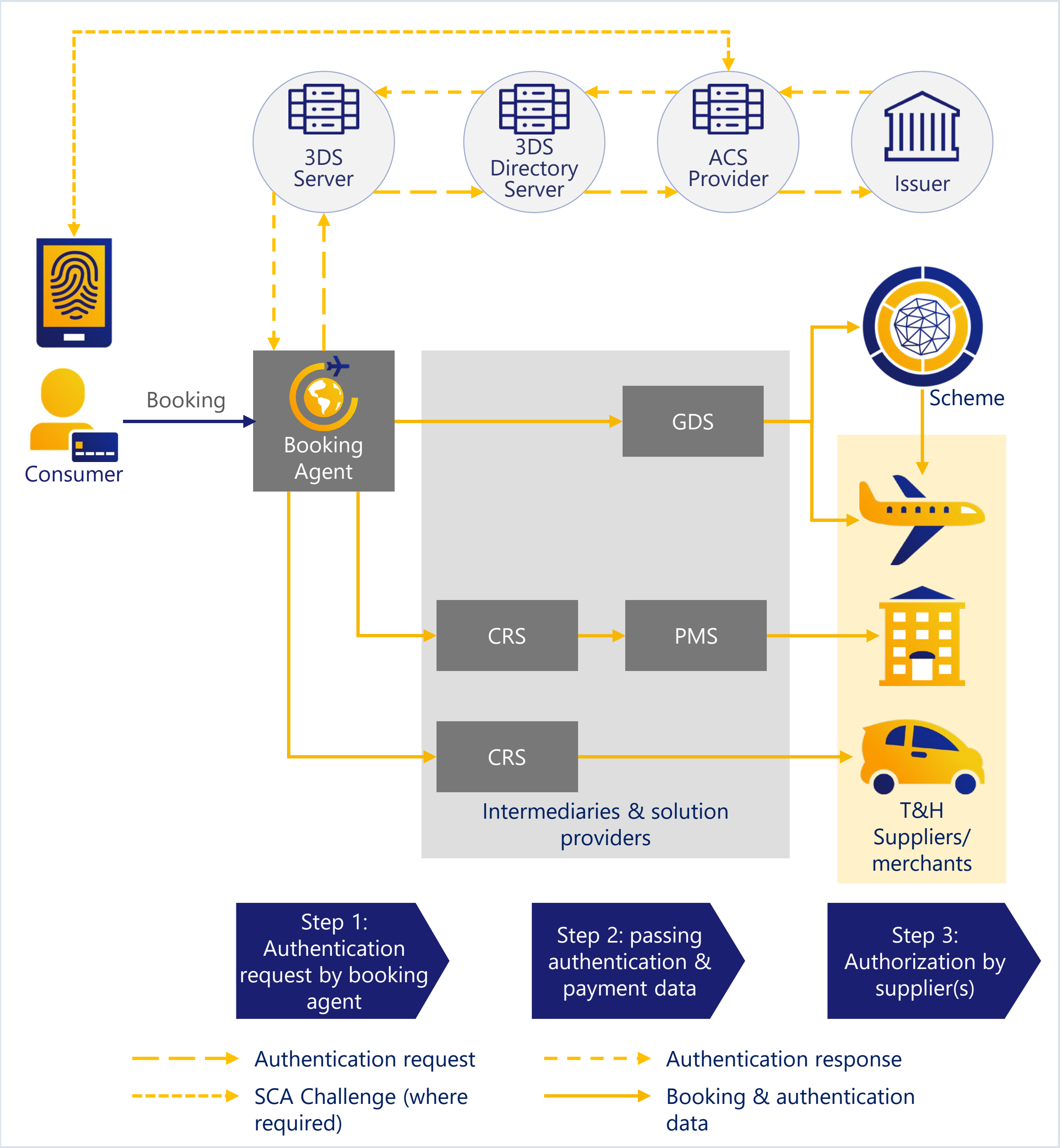
In indirect scenario options where:

- The booking agent requests authentication and the T&H supplier acts as the merchant (option 3 as described in section 4.3), or
- The booking agent requests authentication and both the booking agent and the T&H supplier act as merchants (option 4 as described in section 4.4)

and where the transaction is in scope of SCA and requires authentication at time of booking, the booking agent requests authentication through EMV 3DS, and then passes the authentication data to the T&H supplier(s) enabling them to submit the CIT authorization request(s) with the authentication data (the CAVV, or TAVV in the case of a token transaction and the ECI value). In the case where the booking is processed through an intermediary, this data is passed via the intermediary as shown in Figure 8 below:

[29] For more details please refer to *PSD2 SCA for Remote Electronic Transactions Implementation Guide*

Figure 8 High level authentication, data distribution and authorization flow for an indirect booking where authentication takes place at time of booking for a single merchant


3DS Server
3DS Directory Server
ACS Provider
Issuer
Booking
Consumer
Booking Agent
GDS
Scheme
CRS
PMS
CRS
Intermediaries & solution providers
T&H Suppliers/ merchants
Step 1: Authentication request by booking agent
Step 2: passing authentication & payment data
Step 3: Authorization by supplier(s)
Authentication request
Authentication response
SCA Challenge (where required)
Booking & authentication data

The key principles defined in section 3 apply to the authentication flow. The following additional considerations also apply:

- The entity requesting authentication must communicate the correct booking transaction information to the customer prior to the authentication request including at least the following:
  - The amount the customer will have to pay and when

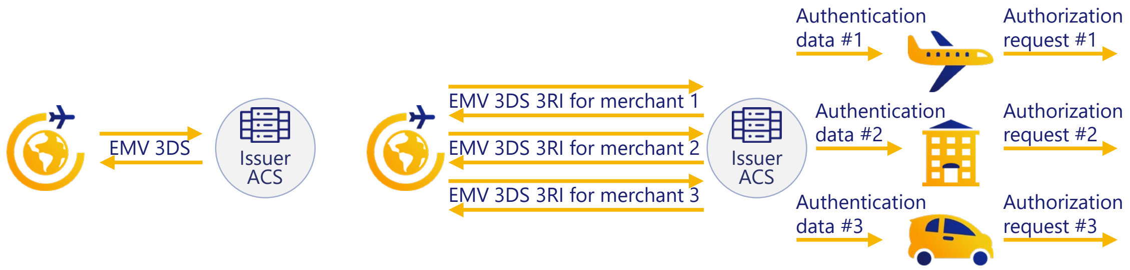
    - How the final amount will be calculated if this is unknown at the time of booking
    - That no charges will appear on their card statement until the order is finalized by each supplier/merchant
    - The merchant name(s) for which authentication is being performed (the merchant name presented must be the name the merchant primarily uses to identify itself to the customer as per Visa Rule #27816)
    - Cancellation and other policies that apply to each service provided by each T&H supplier within the booking (e.g. hotel, airline and car rental)
    - The information that Visa requires to be included in an agreement to set up an MIT (where subsequent payments are going to be collected using MITs). Refer to *PSD2 SCA for Remote Electronic Transactions Implementation Guide* for details
- Merchants who will collect payments via MITs for bookings where the booking agent has requested authentication must update their contractual agreements with their booking agent(s) to request that they perform authentication and disclose the MIT agreement T&Cs

5.2 Requesting Authentication for multiple merchants

If the booking is made via a booking agent on behalf of multiple T&H suppliers[30] who will subsequently submit authorization request(s) and collect payments (options 3 and 4 described in section 4), the process summarised in Figure 9 should be used by the booking agent to enable it to request cardholder authentication only once while ensuring the availability of separate/dedicated authentication data for each party that is to act as a merchant. This process utilises the 3RI feature within EMV 3DS to request the specific authentication data (CAVV) for each individual merchant. Please refer to Appendix A.4 for details on the data required in the initial authentication request versus in the 3RI requests.

[30] Or for itself as a booking agent colleting funds and for a single T&H supplier also collecting funds.

Figure 9: Process for a booking agent requesting authentication for multiple merchants



Step 1: Authentication requested by booking agent

Booking agent requests one authentication for all the suppliers (merchants)

- T&Cs for all merchants must be presented prior to authentication, clearly stating amounts due to each merchant collecting funds
- This single authentication is performed for the total amount due at the time of booking across all suppliers
- The name of agent is the one presented to the customer in the authentication request

Step 2: Requesting authentication data for each merchant

Booking agent requests authentication data (CAVV) for each merchant that needs it via EMV 3DS 3RI

- For each merchant this should include:
  - "Name of agent*name of merchant" and
  - Amount due to that merchant at time of booking or
  - Zero amount if authentication is just setting up future MIT(s)

Interim solution:

- Until 3RI Is fully available in September 2022 the initial CAVV obtained in step 1 may be used maximum of 5 times

Step 3: Authorization requested by merchants

The booking agent passes the merchant specific authentication data (e.g. CAVV & ECI value) to each individual merchant

Each merchant submits its authentication data with its authorization request(s)

Interim solution:

- Until systems can be upgraded to pass authentication data the Interim solution described in section 4.6 may be used

Please note the following:

- If one or more T&H suppliers will subsequently collect payments via MITs, the T&Cs for each merchant must be presented before the authentication request to meet the requirements summarised in section 3.1.1
- While 3RI is the long term solution to be used to request CAVVs for each party that will act as a merchant (including the booking agent if both the booking agent and supplier(s) are collecting funds), as 3RI is not yet fully supported by Issuers, it is not recommended that this option is used until 22 April 2022. Instead, as an interim approach , the CAVV obtained during the initial authentication request can be used in up to a maximum of 5 different authorizations. This interim approach can be used until 31 August 2022. After this date, the 3RI functionality MUST be used to obtain a CAVV for each merchant as described above and in Appendix A.4.
- Refer to Appendix A.4 for more details on the information to include in the initial authentication request vs the 3RI request(s)

If the booking involves merchants processing their own payment and using multiple currencies, (i.e. processing the authorization request in different currencies)

- Cardholders must be displayed the separate amounts they will be requested to pay in the currency to be used by each merchant

- The initial authentication request by the Agent must be done using one single currency for an amount that would cover the total, e.g. in Euros.[31]
- The 3RI request should be in the currency that will be used by each individual merchant (as displayed to the cardholder).

5.3 Authorization Flows

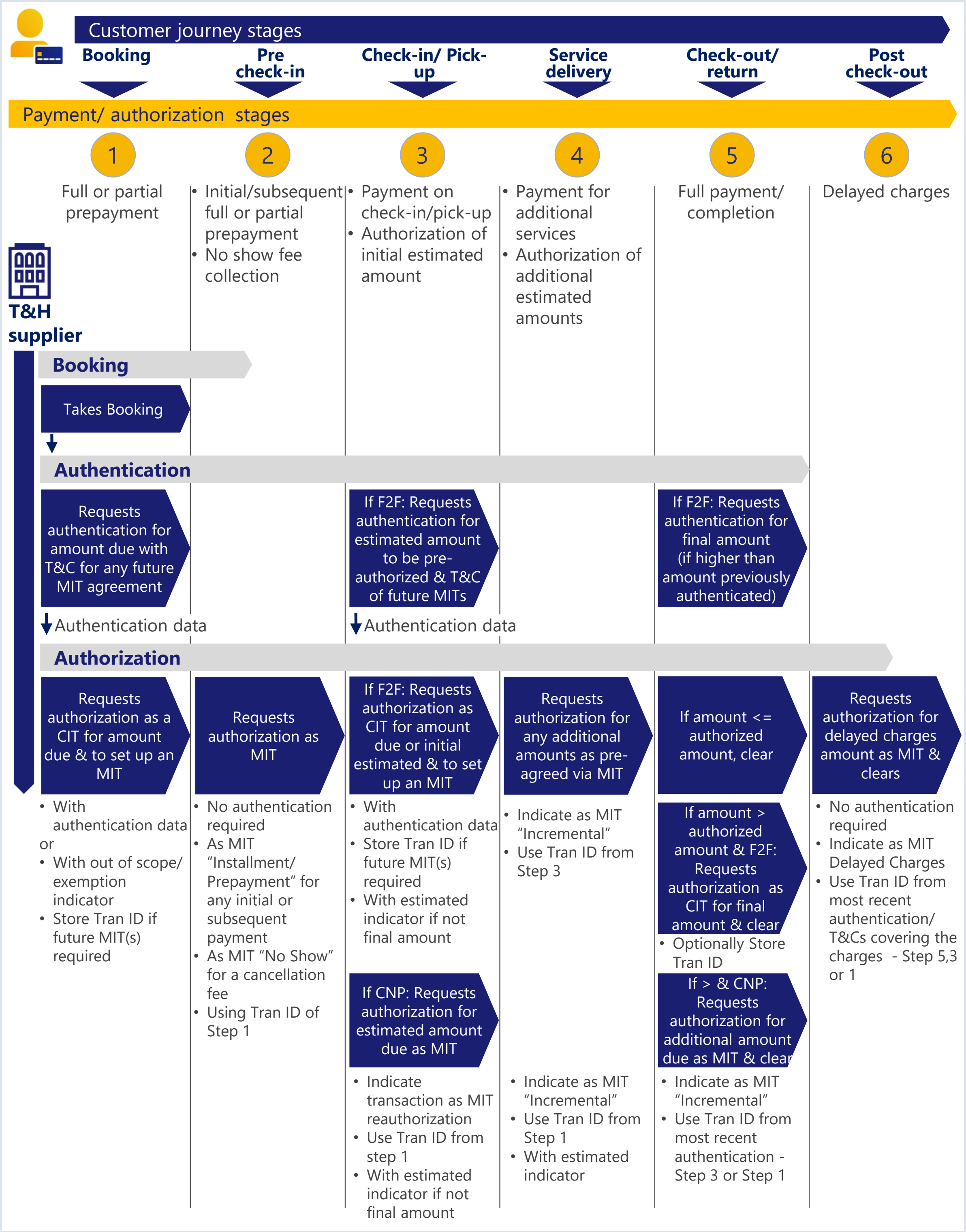
The following flows show the authorization steps for payment types taken at steps 1,2, 3 to 5 and 6 of Figure 7 above for each of the three use cases:

[31] Visa cannot guarantee Issuers will approve if the authentication amount differs from the authorization amount due to a fluctuation in exchange rates.

5.3.1 Direct with the T&H supplier as merchant

In this case, the T&H supplier requests authentication and authorization for all four of the payment types as shown in Figure 10 below:

Figure 10: Authentication & authorization flow for direct booking with T&H supplier as merchant case



Customer journey stages

Payment/ authorization stages

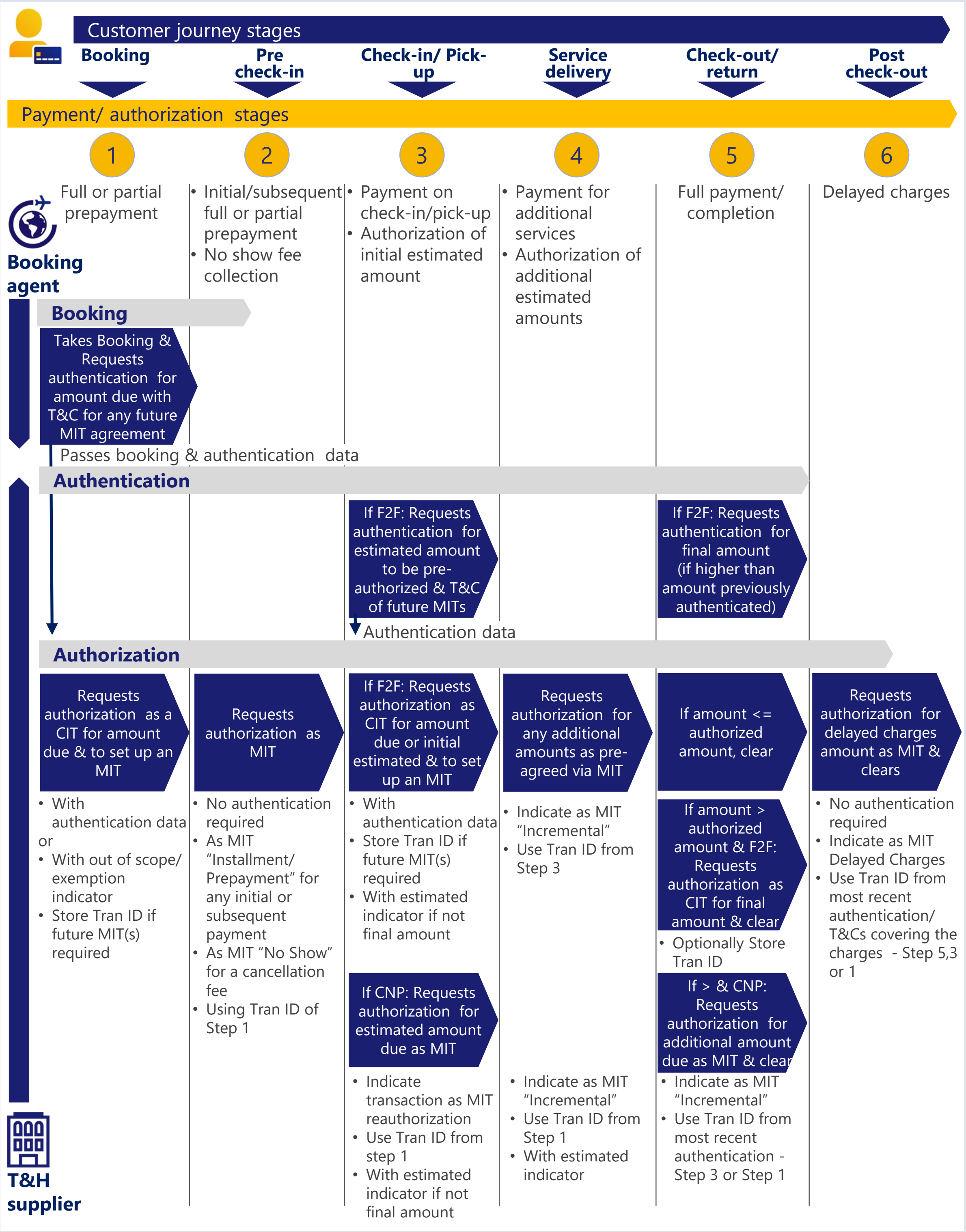
T&H supplier

	Booking	Pre check-in	Check-in/ Pick-up	Service delivery	Check-out/ return	Post check-out
	1	2	3	4	5	6
	Full or partial prepayment	• Initial/subsequent full or partial prepayment • No show fee collection	• Payment on check-in/pick-up • Authorization of initial estimated amount	• Payment for additional services • Authorization of additional estimated amounts	Full payment/ completion	Delayed charges
Booking	Takes Booking					
Authentication	Requests authentication for amount due with T&C for any future MIT agreement Authentication data		If F2F: Requests authentication for estimated amount to be pre-authorized & T&C of future MITs Authentication data		If F2F: Requests authentication for final amount (if higher than amount previously authenticated)	
Authorization	Requests authorization as a CIT for amount due & to set up an MIT • With authentication data or • With out of scope/ exemption indicator • Store Tran ID if future MIT(s) required	Requests authorization as MIT • No authentication required • As MIT "Installment/ Prepayment" for any initial or subsequent payment • As MIT "No Show" for a cancellation fee • Using Tran ID of Step 1	If F2F: Requests authorization as CIT for amount due or initial estimated & to set up an MIT • With authentication data • Store Tran ID if future MIT(s) required • With estimated indicator if not final amount	Requests authorization for any additional amounts as pre-agreed via MIT • Indicate as MIT "Incremental" • Use Tran ID from Step 3	If amount <= authorized amount, clear If amount > authorized amount & F2F: Requests authorization as CIT for final amount & clear • Optionally Store Tran ID	Requests authorization for delayed charges amount as MIT & clears • No authentication required • Indicate as MIT Delayed Charges • Use Tran ID from most recent authentication/ T&Cs covering the charges - Step 5,3 or 1
			If CNP: Requests authorization for estimated amount due as MIT • Indicate transaction as MIT reauthorization • Use Tran ID from step 1 • With estimated indicator if not final amount	• Indicate as MIT "Incremental" • Use Tran ID from Step 1 • With estimated indicator	If > & CNP: Requests authorization for additional amount due as MIT & clear • Indicate as MIT "Incremental" • Use Tran ID from most recent authentication - Step 3 or Step 1	

5.3.2 Indirect booking via the booking agent who handles authentication only

In this case, the booking agent requests authentication on booking and the T&H supplier is the merchant that requests authorization shortly after and requests authentication and authorization at all subsequent stages for all four of the payment types as shown in Figure 11:

Figure 11: Authentication & authorization flow for indirect booking with T&H supplier as merchant case



Customer journey stages

Booking | Pre check-in | Check-in/ Pick-up | Service delivery | Check-out/ return | Post check-out

Payment/ authorization stages

1 Full or partial prepayment

2
- Initial/subsequent full or partial prepayment
- No show fee collection

3
- Payment on check-in/pick-up
- Authorization of initial estimated amount

4
- Payment for additional services
- Authorization of additional estimated amounts

5 Full payment/ completion

6 Delayed charges

Booking agent

Booking

Takes Booking & Requests authentication for amount due with T&C for any future MIT agreement

Passes booking & authentication data

Authentication

If F2F: Requests authentication for estimated amount to be pre-authorized & T&C of future MITs

If F2F: Requests authentication for final amount (if higher than amount previously authenticated)

Authentication data

Authorization

Requests authorization as a CIT for amount due & to set up an MIT
- With authentication data

or
- With out of scope/ exemption indicator
- Store Tran ID if future MIT(s) required

Requests authorization as MIT
- No authentication required
- As MIT "Installment/ Prepayment" for any initial or subsequent payment
- As MIT "No Show" for a cancellation fee
- Using Tran ID of Step 1

If F2F: Requests authorization as CIT for amount due or initial estimated & to set up an MIT
- With authentication data
- Store Tran ID if future MIT(s) required
- With estimated indicator if not final amount

If CNP: Requests authorization for estimated amount due as MIT
- Indicate transaction as MIT reauthorization
- Use Tran ID from step 1
- With estimated indicator if not final amount

Requests authorization for any additional amounts as pre-agreed via MIT
- Indicate as MIT "Incremental"
- Use Tran ID from Step 3
- Indicate as MIT "Incremental"
- Use Tran ID from Step 1
- With estimated indicator

If amount <= authorized amount, clear

If amount > authorized amount & F2F: Requests authorization as CIT for final amount & clear
- Optionally Store Tran ID

If > & CNP: Requests authorization for additional amount due as MIT & clear
- Indicate as MIT "Incremental"
- Use Tran ID from most recent authentication - Step 3 or Step 1

Requests authorization for delayed charges amount as MIT & clears
- No authentication required
- Indicate as MIT Delayed Charges
- Use Tran ID from most recent authentication/ T&Cs covering the charges - Step 5,3 or 1

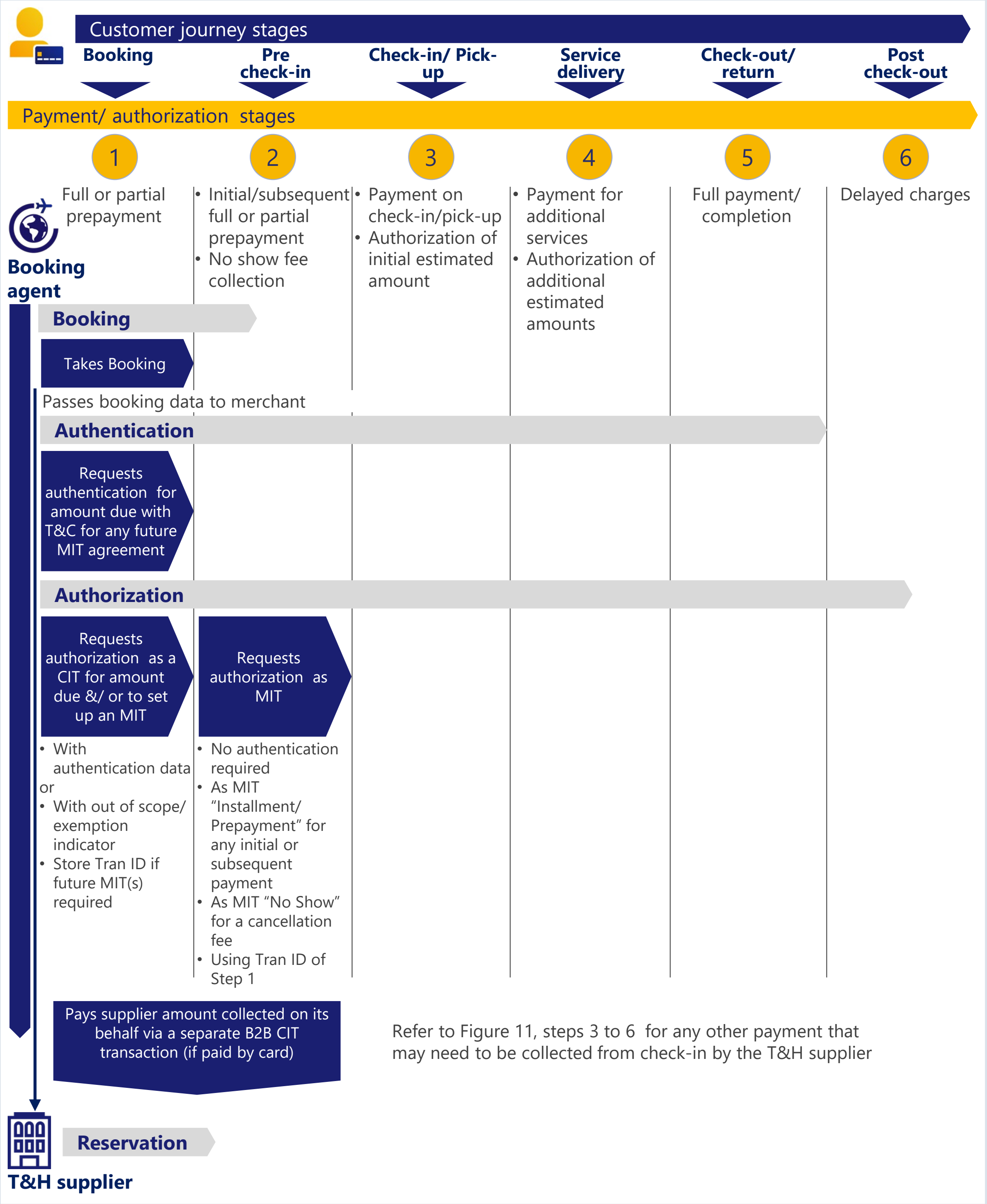
T&H supplier

Version 2.0
24 June 2021

5.3.3 Indirect booking via a booking agent who handles the authentication and authorization requests

In this case, the booking agent requests authentication on booking and acts as the merchant requesting authorization and collecting payment from the customer. The booking agent then pays the T&H supplier through a separate B2B transaction.

Figure 12 : Authentication & authorization flow for indirect booking with booking agent as merchant case - booking agent collects all fees agreed before/at check-in

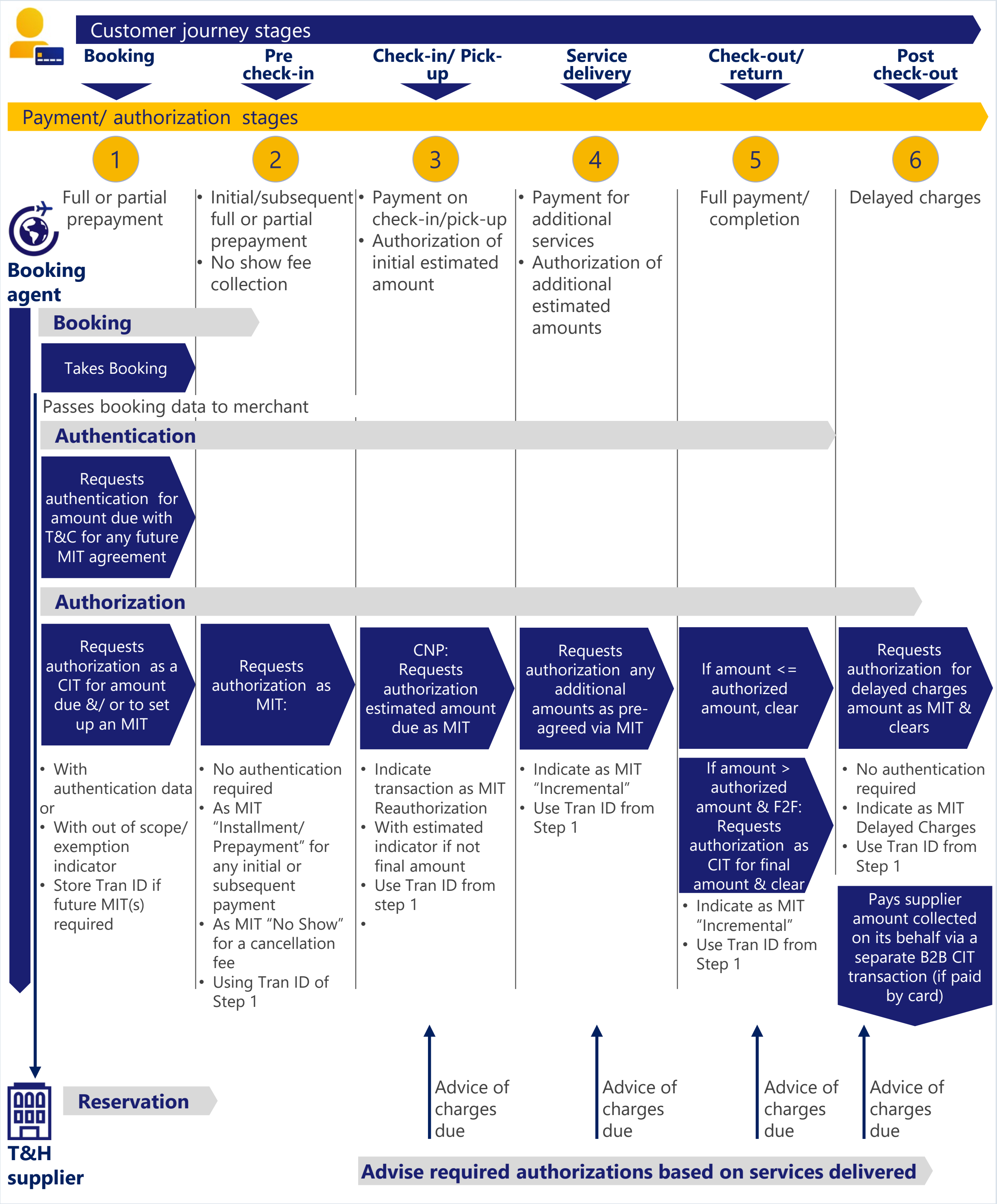


Customer journey stages
Booking
Pre check-in
Check-in/ Pick-up
Service delivery
Check-out/ return
Post check-out
Payment/ authorization stages
1
2
3
4
5
6
Full or partial prepayment
• Initial/subsequent full or partial prepayment
• No show fee collection
• Payment on check-in/pick-up
• Authorization of initial estimated amount
• Payment for additional services
• Authorization of additional estimated amounts
Full payment/ completion
Delayed charges
Booking agent
Booking
Takes Booking
Passes booking data to merchant
Authentication
Requests authentication for amount due with T&C for any future MIT agreement
Authorization
Requests authorization as a CIT for amount due &/ or to set up an MIT
• With authentication data
or
• With out of scope/ exemption indicator
• Store Tran ID if future MIT(s) required
Requests authorization as MIT
• No authentication required
• As MIT "Installment/ Prepayment" for any initial or subsequent payment
• As MIT "No Show" for a cancellation fee
• Using Tran ID of Step 1
Pays supplier amount collected on its behalf via a separate B2B CIT transaction (if paid by card)
Refer to Figure 11, steps 3 to 6 for any other payment that may need to be collected from check-in by the T&H supplier
Reservation
T&H supplier

Generally, the booking agent only collects pre-set charges on behalf of the merchant up to the point of check-in, and any additional incremental amounts for additional services or charges due post check-in will be collected directly by the supplier who will need to ensure a separate authentication is done at check-in to enable any such payment collection via MITs.

Figure 13 below shows the process that should be adopted in the case all payments due throughout where the booking agent requests authentication at the time of booking and are also collected by the booking agent in order to enable express check-in/check-out. This allows the booking agent to collect on behalf of the T&H supplier all agreed prepayments and no show fees and, subject to applicable T&Cs being agreed to by the customer at authentication, any incremental fees incurred during a stay. The booking agent would subsequently make a separate B2B payment to the T&H supplier for the amount owing, typically using a commercial virtual card, bank transfer or Visa Direct payment. This use case does however rely on the supplier being able to inform the booking agent every time additional services are provided to the client and payment needs to be collected during the stay. This is not currently a commonly adopted model, but is feasible as long as all customer T&Cs and appropriate supplier/booking agent agreements are in place.

Figure 13: Authentication flow for indirect booking with booking agent as merchant case – booking agent only collects all fees even additional fees that may occur during a stay



Customer journey stages

Booking | Pre check-in | Check-in/ Pick-up | Service delivery | Check-out/ return | Post check-out

Payment/ authorization stages

1 Full or partial prepayment

2
- Initial/subsequent full or partial prepayment
- No show fee collection

3
- Payment on check-in/pick-up
- Authorization of initial estimated amount

4
- Payment for additional services
- Authorization of additional estimated amounts

5 Full payment/ completion

6 Delayed charges

Booking agent

Booking

Takes Booking

Passes booking data to merchant

Authentication

Requests authentication for amount due with T&C for any future MIT agreement

Authorization

1: Requests authorization as a CIT for amount due &/ or to set up an MIT
- With authentication data

or
- With out of scope/ exemption indicator
- Store Tran ID if future MIT(s) required

2: Requests authorization as MIT:
- No authentication required
- As MIT "Installment/ Prepayment" for any initial or subsequent payment
- As MIT "No Show" for a cancellation fee
- Using Tran ID of Step 1

3: CNP: Requests authorization estimated amount due as MIT
- Indicate transaction as MIT Reauthorization
- With estimated indicator if not final amount
- Use Tran ID from step 1
-

4: Requests authorization any additional amounts as pre-agreed via MIT
- Indicate as MIT "Incremental"
- Use Tran ID from Step 1

5: If amount <= authorized amount, clear

If amount > authorized amount & F2F: Requests authorization as CIT for final amount & clear
- Indicate as MIT "Incremental"
- Use Tran ID from Step 1

6: Requests authorization for delayed charges amount as MIT & clears
- No authentication required
- Indicate as MIT Delayed Charges
- Use Tran ID from Step 1

Pays supplier amount collected on its behalf via a separate B2B CIT transaction (if paid by card)

Advice of charges due

Advice of charges due

Advice of charges due

Advice of charges due

T&H supplier

Reservation

Advise required authorizations based on services delivered

6. Stakeholder checklists

This section highlights the key actions that booking agents and travel and hospitality suppliers/merchants, and their Acquirers & Issuers should consider taking to ensure they are ready for PSD2 SCA.

6.1 Checklist for booking agents

Action		Key points
1	**Discuss with suppliers whose bookings you handle how they would like transaction authentication/authorization requested.**	• Depending on whether the merchant selects option 1, 2 3 or 4 explained in section 4.5.1 the different actions/systems upgrade you will have to take to support each booking will differ.
2	**Ensure authentication can be requested on booking**	• Be ready to request authentication on behalf of T&H suppliers, or to handle authentication and authorization as a merchant • For e-commerce transactions, be ready to support EMV 3DS 2.2 which supports: • 3RI to enable authentication on behalf of multiple merchants at a time and • Exemption indicators to minimise customer friction • In the case of Face to face bookings, transactions must be authenticated using Chip & PIN, or contactless with CVM. In most cases this means you will have to collect the funds on behalf of the supplier as there is no readily available solution to pass chip and PIN data to the supplier to enable them to request authorization for a transaction • If it is not possible to request authentication on behalf of a supplier and provide them with the proof of authentication, consider providing the customer with a link to pay directly via the supplier's website
3	**To support option 3 and 4 described in section 4, you need to work with intermediaries to ensure they upgrade their systems to allow the passing of required authentication and transaction data to merchants**	• Under Options 3 and 4, the booking agent requests authentication and the T&H supplier is the merchant for all or part of the payment. • For more guidance on the system upgrades required to support these options see Appendix A.3 • System upgrades are not necessary for Options 1 or 2 when the same party requests authentication and collects payment

Action		Key points
4	**If you support corporate bookings via a secure corporate payment process be ready to support the SCP exemption**	- Refer to checklist guidance for TMCs and Corporate Booking Tools CBT section below. - It is still recommended that SCA is supported for when this exemption may not apply.

6.2 Checklist for TMCs and Corporate Booking Tools

Action		Key points
1	**Ensure you can request authentication on any in-scope transactions where the SCP exemption cannot be applied by the Issuer**	- Even if you use secure processes where the SCP exemption may generally apply, there will be circumstances where the exemption cannot be applied and SCA will be required or requested by an Issuer. For example: - The exemption can only be used for eligible cards and you may not always be able to determine that a card is eligible and may have to request authentication. - An Issuer may not support the SCP exemption and so may request authentication when the authorization request is submitted. In the case of a T&H supplier collecting a deposit or no show payment this may be some time after booking - In order to minimise declines, TMCs and CBTs should: - Establish processes with customers to take account of the potential need to apply SCA, or to exclude non-qualifying cards from your processes - Check whether an Issuer supports the SCP exemption for the card being used at the time of booking time by submitting the transaction via EMV 3DS - For more detailed guidance please refer to the *PSD2 SCA Secure Corporate Payment Exemption Guide*

Action		Key points
2	**Ensure sufficient security controls are in place for systems that are used to process booking payments on behalf of corporate customers**	• If transactions initiated through your systems are to qualify for application of the SCP exemption by Issuers, they will as a minimum need to offer equivalent levels of security to the application of SCA • Not putting in place security controls is not sufficient in its own right to allow application of the SCP exemption. NCAs must be satisfied that the requirements of the regulation are met before the exemption can be used • Refer to the *PSD2 SCA Secure Corporate Payment Exemption Guide* for more information on the requirements for applying the SCP exemption
3	**Ensure the SCP exemption framework of controls is in place if you want the Issuer to apply the SCP exemption to transactions originated within your system**	• Ensure agreements referred to in the framework are in place with your corporate customers and suppliers as detailed in the *PSD2 SCA Secure Corporate Payment Exemption Guide*
4	**Put in place secure connections with any merchants that you currently book via their public websites – unless it is possible to authenticate each transaction with SCA**	• TMCs / Aggregators cannot benefit from the Issuer applying the SCP exemption when bookings are made via public merchant websites (including through screen scraping) • Review connections with all merchants. • Putting in place secure booking APIs in place of manual booking or screen scraping • Ensuring that the merchant can identify that bookings made via an API originate from a secure system eligible for the SCP exemption • When this is not the case, be ready to support SCA
5	**Discuss with intermediaries to ensure they upgrade their systems to allow the passing of the info about potential qualification for application of the SCP exemption and the required authentication and transaction data to merchants**	• For more detailed guidance please refer to AppendixA.3.

6.3 Checklist for Global Distribution Systems (GDSs)

Action		Key points
1	**Stop flagging all authorization requests as MOTO by default, by the enforcement date**	• Process e-commerce with full authentication data when the booking originates in the e-commerce channel • Only use the MOTO indicator where: • The transaction is initiated via mail/telephone, or: • The transaction is the result of an indirect sale, and the cardholder has been authenticated, however a party in the booking chain is not ready yet to send you the authentication data (MOTO interim solution see section 4.6 for more information) • To achieve this, GDSs must ask their booking agent partners for more information about the context of interaction with the cardholder and must ensure that the transaction has been authenticated when required
2	**Only use the SCP exemption indicator when the transaction originated from an eligible TMC/CBT who can confirm that the context of interaction with the client justifies using this exemption**	• Where the TMC/CBT is not ready to send this information, the MOTO indicator may be used as a limited interim solution (see section 4.6 for more information).

6.4 Checklist for T&H suppliers and booking agents who act as merchants

Action		Key points
Analyse & strategize:		
1	**Impact-assess all transaction use-cases**	• Review your options, summarised in section 4 for compliance for indirect sales
2	**Understand your end-to-end processing infrastructure**	• Review relevant solutions, networks and protocols in scope of change, and engage with booking and payment channels and partners to ensure that authentication data can be received and/or payments can be processed in line with the PSD2 SCA regulation.
3	**Develop authentication and authorization strategies that suit your desired business model**	• Reach alignment with your suppliers and sales channel partners on the upgrades they must make to support this • This is relevant to all sales channels and may impact all intermediaries in the chain including: • OTAs, TMCs, CRSs, PMSs, GDSs, POS vendors
4	**Prioritise the work within your business**	• Ensure the funding and resources are available to implement the required changes
Implement & Optimise		
5	**Implement EMV 3DS 2.2 where SCA needed**	• Review how/when exemptions can be used (cannot be used when setting up MITs) • Ensure your fraud and risk tools maintain fraud rates within target reference rates if you want to take maximise your ability to benefit from exemptions

Action		Key points
6	**Update POS systems to ensure that all transactions are flagged appropriately**	• Limit use of the MOTO indicator to transactions: ◦ Originating through a telephone or mail booking channel, and ◦ MITs that are the result of in indirect sales where it is necessary to use the interim MOTO indicator solution until MIT indicators can be passed through the booking chain • Note that the interim solution is only temporary and work to upgrade should commence as soon as possible if it has not already started • Ensure MITs after booking can be processed with appropriate proof of authentication. This means a CIT authorization request must be submitted with authentication data within 72 hours of booking and if MITs could be processed prior to check-in, the Tran ID of this CIT must be stored. • For any CNP payment after check in: ◦ Ensure MIT agreements are presented and authenticated either at booking or at check-in ◦ Ensure the point of sale system can store the Tran ID of the CIT where the agreement was made ◦ Process each of these MIT payments with appropriate MIT flagging: ▪ Correct MIT type depending on the type of payment collected ▪ Tran ID of the CIT
7	**Update contracts as appropriate**	For example, with: • Your Acquirer for the appropriate use of the MOTO flag if required • With booking agents & intermediaries where they need to, for example, request authentication, indicate exemptions, present T&Cs and/or pass authentication data on your behalf

Action		Key points
8	**Review check-in desk and app procedures**	• Update T&Cs to include MITs if required (in-app, front desk, loyalty scheme) to cover delayed charges and damages • Ensure front and back office staff are aware of any changes to policies & procedures, including the potential need to take card details and request authentication at check-in if further charges may be required that were not covered by the T&Cs and authentication at booking

6.5 Checklist for Acquirers & Gateways

Action		Key points
1	**Communicate impacts to your T&H sector merchants (and their intermediaries where possible)**	• There is still low awareness of how each of their payment processes/needs is impacted
2	**Ensure you can support the "MOTO" indicator interim solution for MITs**	• Upgrade contract with relevant merchants and put appropriate monitoring in place • Ensure the MOTO flag is actually populated in the transaction where appropriate
3	**Ensure your solutions at POS support MITs**	• For No Show, Incremental, Delayed charges, Reauthorization
4	**Ensure you are ready to support the SCP exemption indicator where this exemption may apply**	• Ensure contract/controls in place with eligible merchants • Ensure the SCP exemption indicator can be passed to Issuers
5	**Consider what solutions you have to support T&H merchants**	Examples could include: • Integrated POS solutions enabling integration of on-line bookings with check-in desk systems • Discuss with your merchants how to provide a "payment link" option to their booking agent partners or a redirection to the merchant's own payment page so that the client can be invited to pay directly there when the merchant selects option 1 described in section 4 to handle SCA

6.6 Checklist for Issuers

Action		Key points
1	**Be ready to handle the MOTO indicator as out of scope**	• Volume of MOTO transaction may increase as Travel & Hospitality merchant adopt the Interim solution to MIT flagging
2	**Decide how to handle merchant key entered transactions from the T&H sector that have no MOTO indicator**	• These transactions likely represent MITs from merchant that are not yet ready to support SCA and/or the interim solution. Issuers should consider regulatory requirements and the desire to support business continuity/cardholder experience as well as apply regular risk-based analysis when deciding whether to accept or decline such transactions. Issuers are also recommended to apply exemptions where applicable.
3	**Be ready to support the SCP exemption**	Refer to the guidance given in *PSD2 SCA Secure Corporate Payment Exemption Guide.* In summary: • Follow your National Competent Authority (NCA)'s requirements for usage of this exemption • Recognise Virtual & CTA/Lodged cards via account range (transactions with those cards may not have the SCP indicator) • Have your authorization policies ready for the SCP exemption indicator

7. Bibliography

The following documents provide additional detailed guidance as described in the text of this guide. Note the version/date given for Visa documents is the current version at the time of publication of this guise. Readers should check that they refer to the latest version available on Visa Online.

Table 5: Bibliography

Document/Resource	Version/Date	Description
COMMISSION DELEGATED REGULATION (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication	13 March 2018	The PSD2 Regulatory Technical Standards (RTS) published by the European Banking Authority (EBA) that establishes the requirements to be complied with by payment service providers for the purpose of implementing security measures which enable them to comply with the security requirements of the PSD2 legislation.
Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC	EBA-Op-2018-04 13 June 2018	EBA opinion paper clarifying various RTS requirements notably on the application of exemptions
EBA Q&A		EBA Online Q&A Tool that provides answers to specific questions raised by interested stakeholders. This is available at https://eba.europa.eu/single-rule-book-qa/qna/view/publicId
PSD2 SCA for Remote Electronic Transactions Implementation Guide	Version 3.0 Jan 2021	Comprehensive Implementation Guide providing practical guidance on implementing SCA and Visa solutions.
PSD2 SCA Regulatory Guide	Version 1.0 December 2020	Summarises the main requirements of the PSD2 SCA regulation as it applies to electronic card payments and Visa's guidance on the practical application of SCA in a PSD2 environment. The guide aims to provide a clear single point of reference providing guidance on interpreting the regulation.

Document/Resource	Version/Date	Description
PSD2 SCA Commercial Cards Guide	Version 1.1 March 2021	Provides Issuers of Commercial Cards with guidelines on the application of SCA and the other exemptions defined in the PSD2 SCA RTS to remote electronic transactions performed with Commercial Cards. It also summarises guidance that Issuers may wish to give to their Commercial Card customers to ensure that transactions are not unnecessarily declined due to the inability to apply SCA.
PSD2 SCA Secure Corporate Payments Exemption Implementation Guide	Version 1.2 June 2021	Contains more detailed guidance on the application of the secure corporate payments (SCP) exemption.
PSD2 SCA Optimisation Best Practice guide	July 2020	This guide provides merchants, Acquirers and Issuers with guidance on minimising the number of transactions that will require Issuers to apply SCA challenges.
PSD2 SCA Challenge Design Best Practice Guide	July 2020	This guide provides merchants, Acquirers and Issuers with guidance on minimising friction when SCA challenges are required.
PSD2 Strong Customer Authentication for Remote Electronic Commerce Transactions – European Economic Area: Visa Supplemental Requirements	Version 2.0 December 2020	Guide summarizing Visa Rules relevant to the application of PSD2 SCA.
EMVCo 3-D Secure Specification	V2.2	Specification for the core 3DS technology that includes message flows, field values etc. available at: https://www.emvco.com/emv-technologies/3d-secure/
UK Finance communication on requirements for Strong Customer Authentication – Travel & Hospitality – Indirect Bookings Technical Readiness	December 2020	Guidelines developed by industry stakeholders under the UK Finance umbrella 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 guidance aligns with the guidance given in Appendix A.3 of this document

Glossary

Table 6: Glossary of terms

Term	Description
1-9	
3-D Secure (3DS) 2.0	The Three Domain Secure (3-D Secure™ or 3DS) Protocol has been developed to improve transaction performance online and to accelerate the growth of e-commerce. The objective is to benefit all participants by providing Issuers with the ability to authenticate customers during an online purchase, thus reducing the likelihood of fraudulent usage of payment cards and improving transaction performance. Visa owns 3DS 1.0.2 and licenses it to other payment providers. EMVCo owns EMV 3DS. Visa's offering of 3DS is called Visa Secure.
A	
Access Control Server (ACS)	A server hardware/software component that supports Visa's EMV 3DS Program and other functions. The ACS is operated by the Issuer or the Issuer's processor. In response to Visa Directory Server inquiries, the ACS verifies that the individual card account number is eligible for authentication, receives authentication requests from merchants, authenticates the customer, and provides digitally signed authentication response messages (containing the authentication results and other Visa's EMV 3DS Program data) to the merchant.
Authentication	Authentication allows the Issuer to verify the identity of the cardholder or the validity of the use of the card, including the use of the cardholder's personalized security credentials and, where required, takes place before authorization, using the Issuer's selected authentication method, which in most cases will be 3-D Secure. The term "authentication" is used in this guide to refer to the authentication process flow through which an agent or merchant requests authentication and which may result in either the application of an SCA challenge or of an exemption.
Authorization	Authorization determines if a specific transaction request receives an approval or a decline from the issuing bank, or from VisaNet standing in on the issuing bank's behalf. Once a cardholder initiates a purchase, VisaNet informs the Issuer of the transaction, and receives back their approval or decline

Term	Description
	response. VisaNet then informs the requestor of the response, who passes the information along to the Merchant.
C	
Central Travel Account (CTA) or Lodged Account (sometimes also referred to as "Ghost Cards")	A card account that is issued to a corporate customer (a company or organization), not an individual, and is typically: • Held by an agent, such as a Travel Management Company (TMC), approved by the corporate customer to make authorised travel purchases or bookings on behalf of the corporate customer, or: • Lodged/embedded directly with a merchant by the corporate customer and used by the merchant to charge for agreed goods and services ordered by the customer No physical card is issued. The CTA allows purchases to be initiated on behalf of the corporate customer while the payment transaction takes place directly between the corporate customer and the supplier of the goods or services being provided.
Commercial Card	A Visa Card or a Virtual Account issued to a Client Organization for business-related purchases, as specified in the Visa Rules, and associated with a BIN, account range, or an account designated as one of the following: • Visa Corporate Card • Visa Business Card • Visa Purchasing Card
Corporate Booking Tool (CBT)	A secure software system used by corporates to enable authorized employees to make corporate travel bookings
Customer Reservation System (CRS)	Software platform or system that connects hotels and other travel & hospitality suppliers to TMCs, travel agents and online booking sites, enabling the supplier to receive and manage reservations
D	
Delegated Authentication	Issuers can delegate authentication to an Acquirer and in turn their qualified Delegates. Visa Delegated Authentication provides the framework and conditions for Issuers within the Visa ecosystem to delegate authentication to Delegates that meet stringent qualification criteria.
Direct Bookings	Direct bookings are defined as bookings in which the customer makes the booking directly with the travel or hospitality (T&H)

Term	Description
	supplier via the supplier's own website (or reservation desk) and where the T&H supplier is the merchant collecting payment. An example would be booking a flight directly via an airline's own website.
Directory Server (DS)	An EMVCo 3DS server component operated in the Interoperability Domain; it performs a number of functions that include: authenticating the 3DS Server, routing messages between the 3DS Server and the ACS, and validating the 3DS Server, the 3DS SDK, and the 3DS Requestor.
Dispute	A Transaction that an Issuer returns to an Acquirer.
E	
Electronic Commerce Indicator (ECI)	A value used in an electronic commerce transaction to indicate the transaction's level of authentication and security.
Exemption	The PSD2 SCA RTS provides a number of exemptions to SCA, which could result in minimizing friction and attrition in the customer payment journey. These are: • Low value exemption • Recurring payment exemption • Trusted beneficiaries exemption • Secured corporate payment exemption • Transaction Risk Analysis
G	
Global Distribution System (GDS)	An entity that aggregates and distributes flight schedule and ticket data and booking processes between airlines, travel agents, TMCs and CBTs and requests authorization for card transactions on behalf of merchants. May also aggregate data and bookings for hotels and other travel service suppliers.
I	
Indirect Booking	Indirect bookings are defined as bookings made via a booking agent acting on behalf of a supplier. Examples include a booking for a flight, or a hotel room made via an OTA or when a hotel or car rental booking takes place on the corporate website of the company brand but where the transaction is processed via the franchisee as the merchant.

Term	Description
L	
Liability	Any and all damages (including lost profits or savings, indirect, consequential, special, exemplary, punitive, or incidental), penalties, fines, expenses and costs (including reasonable fees and expenses of legal and other advisers, court costs and other dispute resolution costs), or other losses.
Lodged Account	See Central Travel Account (CTA) and Lodged Accounts
M	
Merchant Initiated Transaction (MIT)	A transaction, or series of transactions, of a fixed or variable amount and fixed or variable interval governed by an agreement between the cardholder and merchant that, once agreed, allows the merchant to initiate subsequent payments without any direct involvement of the cardholder. A transaction can only be an MIT if the cardholder is not available to (I) initiate; or (II) authenticate the transaction. If the cardholder is available to either initiate or authenticate, the transaction is not an MIT.
P	
Primary Account Number (PAN)	The Primary Account Number (PAN) is the number embossed and/or encoded on payment cards and tokens that identifies the card Issuer and the funding account and is used for transaction routing. PAN normally has 16 digits but may be up to 19 digits.
Property Management System (PMS)	Software platform or system that connects hotels to TMCs, travel agents and online booking sites, enabling the hotel to receive and manage reservations and manage the day-to-day operations of the hotel property.
PSD2	The Second European Payment Services Directive whose requirements include that Strong Customer Authentication is applied all electronic payments where both Issuer and Acquirer are within the European Economic Area (EEA). This requirement is effective as of 14 September 2019[32].

[32] The European Banking Authority (EBA) has recognized the need for a delay in enforcement to allow time for all parties in the payments ecosystem to fully implement Strong Customer

Term	Description
PSP	In the context of PSD2, Regulated PSPs are responsible for the application of SCA and of the exemptions. In the case of card payments, these PSPs are Issuers (the payer's PSP) or Acquirers (the payee's PSP).
R	
Regulatory Technical Standards (RTS)	An RTS is a standard that supplements an EU directive. An RTS is developed for the European Commission, in the case of PSD2 by the European Banking Authority (EBA) and is then adopted by the Commission by means of a delegated act. The PSD2 SCA RTS, (formally titled *Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication*) establishes the requirements to be complied with by payment service providers for the purpose of implementing security measures which enable them to comply with the security requirements of the PSD2 legislation.
Risk Based Authentication (RBA)	Risk Based Authentication (RBA) is a process that may be used by Issuers to risk assess and score 3DS transactions to reduce the volumes that require SCA. RBA uses transaction data to assess fraud risk without the need for the cardholder to complete a SCA challenge. RBA is an integral element of EMV 3DS and enables "frictionless" authentication of low risk transactions.
S	
Stored Credential	Information (including, but not limited to, an Account Number or payment Token) that is stored by a merchant or its agent, a Payment Facilitator, or a Staged Digital Wallet Operator to process future Transactions. A credential is not considered a stored credential when the merchant or its agent, Payment Facilitator, or Staged Digital Wallet Operator stores the credential to complete a single transaction or a single purchase for a cardholder (including multiple authorizations related to that particular transaction). For example, when a cardholder provides a payment

Authentication (SCA). Merchants and PSPs should check with NCAs for enforcement timescales in their respective markets.

Term	Description
	credential to a hotel/care rental to cover future reservations and charges as part of the cardholder's membership profile, it is considered a stored credential. However, when the cardholder provides the payment credential to a hotel/car rental to cover charges related to a specific reservation/stay only, it is not.
Strong Customer Authentication (SCA)	SCA, as defined by PSD2 SCA RTS, requires (among other things) that the payer is authenticated by a PSP through independent factors from at least two of the categories of knowledge, possession and inherence. The term "SCA" - is used in this guide to refer to the application of a Strong Customer Authentication (SCA) challenge when such a challenge is required.
T	
Transaction Risk Analysis (TRA) Exemption	Under the Transaction Risk Analysis (TRA) exemption, PSPs may bypass SCA for remote transactions provided risk analysis is applied and the PSP's fraud rates, and transaction amounts are under certain thresholds (Article 18 of the PSD2 SCA RTS). The formula to calculate the PSP's fraud rate for the application of the TRA exemption is total value of unauthorized and fraudulent remote card transactions divided by the total value of all remote card transactions.
Travel Management Company (TMC)	A travel booking agent exclusively making travel bookings on behalf of contracted corporate customers.
V	
Virtual Card	Typically, a single use or limited multi-use card number with an expiry date and security code, that is issued to a designated and authorized user acting on behalf of a corporate purchaser for a business to business transaction initiated through a secure electronic purchasing system. The virtual card number will typically have other restrictions applied to it such as a maximum transaction value that corresponds to the purchase amount and will be limited to use with a single defined merchant or merchant category. No physical card is issued. Please note that "virtual card" is a general term that may include either real card numbers (PANs) or tokens. In either case the virtual card use case is focused on the temporary nature of the card, the controls and security that surround its usage and the absence of a cardholder to authenticate.

Term	Description
	Virtual Commercial Cards are typically used where it is efficient for a merchant to receive B2B payments via individual card transactions rather than bulk invoicing and settlement. Three examples are: • Travel agencies settling booking payments with hotels, • Delivering virtual cards to employee’s mobile device to enable them to pay for an urgent expense when they don’t have a card of their own, and Corporates paying a supplier for an invoiced amount for goods/services rendered.

A Appendices

A.1 Appendix 1: Inclusion of authentication-related data

A merchant and/or Acquirer must populate authorization messages with the correct authentication-related data to indicate to the Issuer one of the following:

- SCA has been performed, or
- An SCA exemption is being exercised, or
- SCA has not been performed or attempted and an exemption is not being exercised, for example, because the transaction is out of scope of SCA.

If a merchant, or Acquirer, fails to include the correct authentication-related data in the authorization for a transaction that is in scope, then the Issuer might decline the transaction, creating unnecessary friction for the cardholder.

This appendix highlights information to help T&H merchants understand which authentication-related data must be populated in the authorization messages for different transaction types, CITs and MITs. It focusses on information that is specifically relevant to the T&H sector. For more general information on authentication related data, defining and flagging CITs and MITs please refer to the *PSD2 SCA for Remote Electronic Transactions Implementation Guide* and whether they qualify for fraud liability protection.

A.1.1 Merchant Initiated Transactions

MITs are out of scope of SCA[33]. Therefore, authentication data is not required in authorization messages for transactions of this type. As such, Issuers may not decline MITs with a response code 1A (SCA required), as the cardholder is not available for authentication during these transactions. The merchant must include the following in the authorization message for transactions of this type:

Table 7 Authentication-related data required for MIT authorization messages

Authentication scenario	Credential type	Exemption Indicator Required	CAVV required	TAVV required	ECI value	Fraud Liability Protection
MIT out of scope	PAN or Token	No	No	No	Various depending on use case and MIT type [34]	Depends in the ECI value

[33] SCA must be performed for the CIT used to set up the MIT agreement in most cases. See Section 3.9 "The Visa MIT Framework" of the *PSD2 SCA for Remote Electronic Transactions Implementation Guide* for full details

[34] The ECI value (Field 60.8) depends on several characteristics of the transaction and does not have a fixed value for transactions where the Visa MIT Framework is used. While in most cases, the ECI value

The key data fields and values for MIT transactions and CITs used to set up MIT agreements are indicated in Table 8 below. The MITs mostly used by the Travel & Hospitality sector are Prepayment/Instalment, No Show, Reauthorization, Incremental and Delayed Charges. But there may be some use cases where the other MITs may be used so all are listed in the table.

Table 8: Key data fields and values for MIT transactions and CITs used to set up MIT Agreements

Description	Transaction Type	Visa MIT Framework			POS Entry Mode (PEM) (F22)	Initiating Party Indicator (F 34[i])	Authentication
		POS environment (F126.13)	Message Reason Code (F63.3)	Original Transaction ID (F125[ii])			
Installment/ Prepayment	First Transaction (CIT) (May be of zero value if set up only)	I	--	--	Any valid[iii] (10 if stored credential)	--	Required
	Subsequent Transactions (MIT)	I	--	Tran ID of first transaction/ previous MIT *(or interim Tran ID)*	10	1[i]	N/A
Recurring	First Transaction (CIT) (May be of zero value if set up only)	R	--	--	Any valid[iii] (10 if stored credential)	--	Required
	Subsequent Transactions (MIT)	R	--	Tran ID of first transaction/ previous MIT *(or interim Tran ID)*	10	1[i]	N/A
Unscheduled Credential on File (UCOF)	First Transaction (CIT) (May be of zero value if set up only)	C	--	--	Any valid[iii] (10 if stored credential)	--	Required

is 07 or 02 there can be several exceptions. Refer to *VisaNet Authorization-Only Online Messages – Technical Specification* for details on possible ECI Values

	Subsequent Transactions (MIT)	C	--	Tran ID of first transaction/ previous MIT *(or interim Tran ID)*	10	1[i]	N/A
Incremental	First Transaction (CIT) (Estimated transaction)[iv]	--	--	--	Any valid[iii] (10 If stored credential)	--	Required
	Subsequent Transactions (MIT)	--	3900	Tran ID of first transaction	Any valid [v] (10 if stored credential)	1[i]	N/A
Delayed Charges	First Transaction (CIT)	--	--	--	Any valid[iii] (10 if stored credential)	--	Required
	Subsequent Transactions (MIT)	--	3902	Tran ID of first transaction *(or interim Tran ID)*	01 or 10 if stored credential	1[i]	N/A
No Show	First Transaction (CIT)	--	--	--	Any valid[iii] (10 if stored credential)	--	Required (except if secure corporate payment exemption applies)
	Subsequent Transactions (MIT)	--	3904	Tran ID of first transaction *(or interim Tran ID)*	01 or 10 if stored credential	1[i]	N/A
Reauthorization	First Transaction (CIT)	--	--	--	Any valid[iii] (10 if stored credential)	--	Exemption may be used. [v] If CAVV available, may or may not be present as the merchant has the option to provide in the initial CIT or in the MIT reauthorization
	Subsequent Transactions (MIT)	--	3903	Tran ID of first transaction	01 or 10 if stored credential		Not required but CAVV may

				(or interim Tran ID)			optionally be present
Resubmission	First Transaction (CIT)	--	--	--	Any valid[iii] (10 if stored credential)	--	Contactless exemption applies[vi]
	Subsequent Transactions (MIT)	--	3901	Tran ID of first transaction *(or interim Tran ID)*	01 or 10 if stored credential	1[i]	N/A

Notes:

i. The new initiating party indicator indicates a transaction is an MIT out of scope of SCA indicator and is populated in Field 34 Tag 80 and is for Issuer use only. Visa will automatically populate the value 1 in Field 34 Tag 80 for Issuer usage when a transaction is submitted by an Acquirer using the existing Visa MIT Framework.

ii. Acquirers may submit the Original Tran ID either in Field 62.2 or in Field 125 Usage 2 DS 03. Visa then forwards this Original Tran ID in Field 125 to the Issuers that participate to receive Field 125. The Transaction ID in F62.2 which is presented in the authorization request to Issuers and response back to Acquirers is the one of the current MIT and not that of the initial CIT as Visa always generates a new, unique, Tran ID for each transaction, including subsequent MITs, in this field (except in the case of incremental authorizations where the initial Tran ID is kept).

iii. Any valid value because these transactions can also originate in F2F channels.

iv. Incremental transactions must be preceded by an estimated/initial authorization. The estimated authorization indicator with a value of 2 or 3 must be included in Field 60.10 - Additional Authorization Indicators.

v. The POS entry mode for MIT Incremental should be the same POS entry mode as the one used in the associated CIT.

vi. The associated subsequent MITs are simply the completion of an existing transaction, no further authentication of the cardholder is required as long as the CIT was compliant, i.e. if exemptions were applicable, they can be used.

A.2 Appendix 2 Eligible MCCs for interim use of MOTO indicator for MITs resulting from indirect sales

Interim use of the MOTO indicator to flag MOTO transactions resulting from indirect sales is restricted to merchants in the MCCs listed in Table 8 below.

Table 9 Eligible MCCs for interim use of MOTO indicator for MITs resulting from indirect sales

MCC Description	MCC
Airlines and Air Carriers	3000 through 3302
Car Rental Agencies	3351 through 3441
Lodging—Hotels, Motels, Resorts	3501 through 3838
Railroads	4011
Local and Suburban Commuter Passenger Transportation, Including Ferries	4111
Passenger Railways	4112
Taxicabs & Limousines	4121
Bus Lines	4131
Steamship and Cruise Lines	4411
Airlines and Air Carriers (Not Elsewhere Classified)	4511
Travel Agencies and Tour Operators	4722
Transportation Services (Not Elsewhere Classified)	4789
Direct Marketing—Insurance Services	5960
Insurance Sales, Underwriting, and Premiums	6300
Real Estate Agents and Managers	6513
Lodging – Hotels, Motels, Resorts, Central Reservation Services (Not Elsewhere Classified)	7011
Trailer Parks & Campgrounds	7033
Automobile Rental Agency	7512
Motor Home and Recreational Vehicle Rentals	7519
Parking Lots, Parking Meters and Garages	7523
Tourist Attractions and Exhibits	7991
Aquariums, Seaquariums, Dolphinariums, and Zoos	7998
Government Services (Not Elsewhere Classified)	9399

A.3 Appendix 3 Data elements that must be passed from booking agents to merchants (directly or by intermediaries)

Table 10 below outlines guidelines developed by industry stakeholders under the UK Finance umbrella on the specific authentication and associated payment data that solution providers and intermediaries should receive and pass on to merchants, following an indirect booking where option 3 or 4 described in section 4 are used. It is provided as guidance for those who need it. Note these data requirements are common across the major card schemes (Visa, MasterCard and American Express).

UK Finance published this guidance in Table 1 of *UK Finance communication on requirements for Strong Customer Authentication – Travel & Hospitality – Indirect Bookings Technical Readiness December 2020*. The difference is that Table 10 below:

1. Has been updated to refer to scenarios as defined in this Visa guide, therefore where the UK Finance document refers to scenario A, and B , this is equivalent to option 3 and 4 respectively in this guide and where UK Finance refers to scenario C this is equivalent to scenarios in the Payment Options column of Table 10 below where transactions are out of scope or where an exemption is used (OOS/E).
2. Indicates when a data element is not required by Visa
3. Provides more detail in the footnotes on when data elements are, or may be required under the option 4 scenario

Disclaimer

This guidance 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. The guidance is intended 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 authorization requests following the enforcement of the SCA requirements stipulated by PSD2 for e-commerce transactions from 31 December 2020 within the EEA and 14 September 2021 in the UK. Although prepared by a UK based working group, the guidance is valid across the world for any stakeholders involved in booking involving UK/EEA issued card and acquired transactions.

While the suggested upgrades are intended to satisfy the requirements of participating schemes, Issuers and Acquirers, Visa does not accept any liability for any actions taken in reliance upon this guidance. 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). If in doubt, merchants and booking agents should check with each of the schemes. Failure to ensure that all necessary and appropriate system upgrades have been made by the enforcement date could result in payment transactions being declined.

While each data element will not be present in each booking, entities should ensure that they can pass all of the data elements defined in the table. They may do this according to their own specification/codes. 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 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 elements defined in the Table 10 may be:

- Required (R)
- Conditional (C)
- Recommended (RM)

and may apply to payment options 3 or 4 as described in section 4.3 and 4.4, or may apply when a transaction is out of scope or qualifies for an exemption (OOS/E)

Table 10: Data elements that must be passed from booking agents to merchants

Data	Field Name	Type & Length	R, C, or RM	Payment Options	Additional Information
1	Card number or Token Number	30 numeric	R	3, 4, OOS/E	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	3, 4, OOS/E	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

Data	Field Name	Type & Length	R, C, or RM	Payment Options	Additional Information
					known, but you may use other agreed industry format to convey this information if available/ appropriate.
3	Card expiry	4 numeric (YYMM)	R	3, 4, OOS/E	
4	CVV2/CVC2 value	Max 4 numeric	RM	3, 4[35], OOS/E	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
5	Channel - One of the following values is required	2 alphanumeric - predetermined values as follows:	R	3, 4, OOS/E	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			

[35] This value is required in option 4 scenarios when the T&H supplier is the party requesting authorization 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 authorization 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

Data	Field Name	Type & Length	R, C, or RM	Payment Options	Additional Information
6	Card or Token number collection method. One of the following values are required	1 alphanumeric – predetermined values as follows:	R	3, 4, OOS/E	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 Indicator 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	3, 4[36], OOS/E	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.
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 request authorization of a payment immediately with the authentication data and will not need to do any MITs.
7.2	Trusted Beneficiary Exemption	"TB"			

[36] This value is required in option 4 scenarios when a T&H supplier is requesting authorization 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 authorization 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.

Data	Field Name	Type & Length	R, C, or RM	Payment Options	Additional Information
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	3, 4, OOS/E	This field describes the agreed mandate (if any) between the cardholder and the booking 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.

Data	Field Name	Type & Length	R, C, or RM	Payment Options	Additional Information
					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 present their 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"			
8.9	Be ready to accept new value that could be created over time	2 alphanumeric			

Data	Field Name	Type & Length	R, C, or RM	Payment Options	Additional Information
9	Identifier of authorization (Authorization Trace ID/Authorization Tran ID)	16 alphanumeric and special characters, values returned from initial authorization response	R	4	This field describes the Transaction ID/Trace ID of the authorization request when submitted by the booking agent. This is not the Directory Server Transaction ID. The Tran ID/Trace ID is only present if an authorization 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 authentication
10	Merchant Name used by authenticator in authentication request	40 alphanumeric characters	C – to be present if requested by the scheme	3, 4, OOS/E	Not requested by Visa
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	C - must be present for all transactions indicated as EC on data element 5.3	3, 4[37]	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

[37] This value is required in option 4 scenarios when a T&H supplier is requesting authorization for a CIT being processed to set up an 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 authorization 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.

.

Data	Field Name	Type & Length	R, C, or RM	Payment Options	Additional Information
		– 20-byte unsigned binary	May optionally be present in other cases (e.g. if Authentication is performed by decoupled authentication for MOTO)		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 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	3, 4[37]	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 token transaction may have been submitted via EMV 3DS and may have both a CAVV and a TAVV. Booking agents will need to pass on the data they receive.
		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 EMV 3DS and have both a CAVV and a TAVV. Booking agents will need to pass on the data they receive.

Data	Field Name	Type & Length	R, C, or RM	Payment Options	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	3, 4	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) EMV 3DS 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	3, 4	Not required by Visa at this time
15	3DS Program Protocol version	3 alphanumeric (no dots in between values)	C - to be present if required by the scheme	3, 4[37]	This may be required in authorization request for certain schemes. Not required for 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) - Recomme	3, 4, OOS/E	It is important to note that when sent for markets where it is not required, it must be correct else better to leave empty.

Data	Field Name	Type & Length	R, C, or RM	Payment Options	Additional Information
			nded in other markets unless market or regional mandate restricts sending this information		
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.			

Data	Field Name	Type & Length	R, C, or RM	Payment Options	Additional Information
		Not required, if state			
		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	OOS/E	
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 authentication issues as they may be created	2 alphanumeric			

Data	Field Name	Type & Length	R, C, or RM	Payment Options	Additional Information
	from time to time				
18	Purchase/ Transaction Amount	12 numeric characters	R	3, 4, OOS/E	
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	3, 4, OOS/E	
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

A.4 Appendix 4. Summary of data required in initial authentication and 3RI requests for travel & hospitality multi-party commerce

Table 11 summarises the data that that is required in the initial authentication and subsequent 3RI requests for travel and hospitality indirect booking transaction scenarios

Table 11: Summary of data required in initial authentication request and 3RI requests for travel & hospitality multi-party commerce use case

	Various Fields	Content
1. Authentication request by a Booking Agent for a Single Travel Merchant Use Case	1.1. Authentication request	
	Merchant Name	Travel Agent Name * Name of merchant
	Acquirer BIN & MID	Travel Agent's Acquirer BIN + MID
	3DS Requestor ID	3DS Server Provider BID * 3DS Server assigned unique ID for Travel Agent
	3DS Requestor Name	Travel Agent Name (only)
	Amount	Total purchase amount due at booking time (if no amount due but need to set up an MIT– zero value)
	1.2 Authorization request	
	Acquirer BIN & MID	Merchant's Acquirer BIN & MID
	Card Acceptor Name	Merchant Name
	CAVV	CAVV obtained in step 1.1 (i.e. containing the following merchant descriptor: Travel Agent Name*Name of merchant
	Amount	Total purchase amount due at booking time (if no amount due but need to set up an MIT: account verification – zero value)
2. Authentication requests by a Booking Agent for Multiple Travel Merchants Use Cases*	2.1 Initial Authentication request	
	Merchant Name	Travel Agent Name
	Acquirer BIN & MID	Travel Agent Acquirer BIN & MID
	3DS Requestor ID	3DS Server Provider BID * 3DS Server assigned unique ID for travel agent
	3DS Requestor Name	Travel Agent Name (only)
	Amount	Total purchase amount due at booking time (total for all merchants)
	2.2 3RI Authentication request(s) – the party providing the authentication service does a 3RI request for each merchant in need of a CAVV to process a CIT/set up an MIT	
	Merchant Name	Travel Agent Name*Name of merchant
	Acquirer BIN & MID	Travel Agent Acquirer BIN & MID
	3DS Requestor ID	3DS Server Provider BID * 3DS Server assigned unique ID for travel agent
	3DS Requestor Name	Travel Agent

	Prior Transaction Authentication Information	Merchants need to ensure that all the below required fields are passed though as a part of the 3RI request(s) and that the data supplied is valid to ensure Issuers can relate this 3RI request(s) to the initial one. For Issuers, 3DS Requestor Prior Transaction Authentication Information (threeDSRequestorPriorAuthenticationInfo) improves risk management and provides secondary evaluation of a previously authenticated transaction.) - Prior 3DS Transaction Authentication Method (threeDSReqPriorAuthMethod): Mechanism used by the Cardholder to previously authenticate to the 3DS Requestor. - Prior 3DS Transaction Authentication Timestamp (threeDSReqPriorAuthTimestamp): The date and time in UTC of the prior cardholder authentication. - Prior 3DS Transaction Reference (threeDSReqPriorRef): This data element contains the ACS Transaction ID for a prior authenticated transaction (this is the ID generated by ACS in the initial authentication).
	Amount	Share of the merchant’s total purchase amount due at booking (if no amount due but need to set up an MIT: account verification – zero value)
	2.3 Authorization	
	Acquirer BIN & MID	Merchant’s Acquirer BIN & MID
	Card Acceptor Name	Merchant Name
	Amount	Share of the merchant’s total purchase amount due at booking (if no amount due but need to set up an MIT: account verification – zero value)
	CAVV*	Permitted until 1 September 2022 CAVV obtained in Step 2.1 (can be used up to a maximum of 5 times) or
		CAVV obtained in Step 2.2 *Note: For this use case of Authentication by a booking Agent for multiple travel merchants, it is not recommended to use this option until Visa confirms wide Issuer support of the 3RI functionality*

*Until 1 September 2022, to enable for full Issuer implementation support of 3RI, step 2.2. may be skipped and the CAVV obtained during the initial authentication request can be used in up to a maximum of 5 different authorizations. After this date, the 3RI functionality MUST be used to obtain a CAVV for each merchant.