Implementing Strong Customer Authentication (SCA) for Travel & Hospitality

February 2019

Version 1.0
27th February 2019

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. Payment Service Providers are encouraged to seek the advice of a competent professional where such advice is required. We encourage clients to contact Visa if they experience challenges due to conflicting guidance from local regulators. Where it makes sense, Visa will proactively engage with regulators to try and resolve such issues.

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 3-D Secure 2.0 (3DS 2.0): When in this document we refer to 3-D Secure 2.0 or 3DS 2.0 this is a generic reference to the second generation of 3-D Secure and does reference a specific version of the EMVCo specification. Some 3-D Secure features are only available under versions 2.1, 2.2 or later of the EMVCo specification. Readers will need to refer to the EMVCo specifications or more detailed guidance being published by Visa for information on which version to support.

Contents

1. Introduction

As the digital economy plays an increasing part in all our lives, it is vital that electronic payments are secure, convenient and accessible to all. Visa aims to provide innovative and smart services to Issuers, Acquirers and merchants, so they are able to deliver best in class payments to Visa cardholders.

The Payment Services Directive 2 (PSD2) aims to contribute to a more integrated and efficient European payments market and ensure a level playing field for Payment Services Providers (PSPs). As such, it introduces enhanced security measures to be implemented by all PSPs.

Visa understands that merchants in different sectors have different business processes. Therefore Visa supports the PSD2 requirements for Strong Customer Authentication (SCA) for all different kinds of scenarios, across a range of merchants including eCommerce merchants, online groceries, subscription services and travel and hospitality.

Many of these scenarios require merchants to initiate payments on the cardholder's behalf at a time when the cardholder is not available to perform authentication. Such transactions are known as Merchant Initiated Transactions (MITs). This paper helps merchants to understand how to support SCA across all scenarios, including MITs.

Visa has already established the MIT Framework to enable Acquirers and Issuers to correctly flag and identify MIT transactions. In order to meet the requirements of PSD2 whilst minimising friction and optimising approval rates, it is essential that the MIT Framework is used to ensure that transactions that do not require SCA can be correctly identified.

Key Point

Merchants and Acquirers must use the MIT framework to accurately identify transactions where the cardholder is not available. If this is not done, Issuers may have no choice but to decline transactions that may otherwise be approved.

Visa's vision for secure, compliant, advanced and convenient electronic payments delivers a good balance between security and consumer convenience.

IMPORTANT NOTE: This document provides guidance on the practical application of SCA in a PSD2 environment. Clients should note that this guide should not be taken as legal advice and the following take precedence over content in this guide:

- **Interpretations of the regulation and guidance provided by local competent authorities**
- **Visa core rules**

- **Technical information and guidance published in EMVCo specs and Visa Implementation guides listed in the bibliography**

Visa recognises that clients have choices and may wish to use alternative approaches, tools and services to those referred to in this guide.

1.1 Audience

This guide is intended for anyone involved in the Travel and Hospitality sector processing transactions in the Visa Europe region. This may include:

- Merchants, their Acquirers and third party agents and vendors looking for guidance on implementing SCA solutions
- Issuers seeking to ensure that they accurately recognise transactions that are in and out of scope of SCA so they can maintain security without their cardholder's experience being unnecessarily disrupted

1.2 Scope

In recognition of the diverse number of scenarios Travel and Hospitality merchants deliver, Visa has produced this guide to explain how to implement SCA solutions in the travel and hospitality sector . Scenarios covered include:

- A Travel Agent acting on behalf of one or more other merchants
- A Travel Agent acting as a merchant
- Transport ticket purchasing
- Hotel and car reservations
- Payments for Hotels, Cruises and rental services

The scenarios presented in this document are relevant to merchants providing SCA with PANs and Tokens using 3-D Secure.

2. Principles for implementing SCA specific to the Travel and Hospitality Industry

Irrespective of the business processes that a merchant uses for eCommerce transactions, there are some fundamental principles that shape the approach a merchant takes to facilitating an authorization. These principles are summarised in Section 4.2 of the *PSD2 SCA for Remote Electronic Transactions Implementation Guide*. The following table summarises additional Visa principles applicable specifically to the travel and hospitality industry.

Additional Principles for Travel Use Cases	Rationale
1. **Transactions which originate in the eCommerce channel should be processed as eCommerce.**	If a cardholder makes a travel booking on the internet/via a mobile app, all associated payment authorizations should be processed as eCommerce transactions. eCommerce transactions are in scope of PSD2 SCA except where a transaction is an MIT (e.g. no Show) or is otherwise out of scope. Exemptions to SCA may apply. This is valid until the booking is completed, or until there is another face-to-face interaction with the cardholder where the card is used. Future transactions should then follow face-to-face requirements.
2. **If a transaction is initiated as MOTO, it is out of scope of PSD2 SCA requirements**	MOTO transactions are out of scope of SCA. A MOTO transaction in the Visa processing system is indicated by: • F25 (value 08) and/or • F60.8 (value 01 or 04). The use of the value "01 – Key entered" in F22 is not sufficient to qualify a transaction as MOTO. Merchants should note that one objective of the regulation is to secure as many transactions as possible to reduce fraud, so there should be effort made in the industry to move away from MOTO and to secure transactions.
3. **The Visa MIT Framework must be used to indicate an MIT as out of scope of PSD2 SCA**	For a merchant initiated transaction to receive authorization while minimising the risk of an Issuer requiring SCA, the transaction must be properly indicated using the MIT Framework. This means that even if the MIT Framework is not mandated for transactions processed with a PAN, it is in a merchant's interest to use it so that transactions that are out of scope of PSD2 can be recognised as such.

Additional Principles for Travel Use Cases	Rationale
4. Card absent transactions are only recognized out of scope of the SCA requirements if indicated as MOTO, one leg out or MITs	The PSD2 SCA requirements recognizes as out of scope: MOTO, MITs and 'one leg out' transactions. Transactions that are key entered in a terminal (i.e. value 01 in F22) without the cardholder being present (i.e. with no authentication) and are not MOTO, MIT or 'one leg out' transactions, run the risk of being declined by Issuers if no exemption applies as nothing indicates nor qualifies these transactions as out of scope. Merchants should ensure they use appropriate coding when processing transactions.
5. A Travel Agent may use exemptions in some cases	PSD2 SCA exemptions can only be applied by PSPs (Acquirers or Issuers). A Travel Agent may only raise exemptions if it has been previously agreed with the merchant's Acquirer that the Travel Agent may do so on the acquirer's behalf. The Acquirer must qualify for any exemptions applied. More information on how this could be achieved will be provided in due course. Exemptions should be used with caution: if the Issuer does not agree with applying the exemption, they may respond with an SCA required decline at a time when the cardholder is no longer available.
6. Exemptions should not be used for travel scenarios where a future MIT may be required	In scenarios where a future MIT may be required, PSD2 SCA exemptions should not be applied as part of the initial CIT. This is because the initial CIT is used to set up the future agreement with the cardholder to process the MIT, and for setting up a new agreement SCA is required in most cases, as described in Section 5.9 of the *PSD2 SCA for Remote Electronic Transactions Implementation Guide*.
7. Travel Agencies (MCC 4722) can facilitate authentication on behalf of other merchants' Acquirers for which they handle bookings	Travel agencies and other travel merchants can facilitate authentication on behalf of other merchants' Acquirers for which they may handle the booking. When doing so, in the 3DS and 3DS/3RI request they must identify themselves with MCC 4722, as they are acting as an agent when authenticating for other merchants' Acquirers. For a full description of other data required in the 3DS request(s) when authenticating on behalf of other merchants' Acquirers, please refer to *Section 3.1 Authentication performed by a Travel Agent on behalf of one single merchant* and *Section 3.2 Authentication performed by a Travel Agent on behalf of several other merchants* below. NOTE: T&E and Rail and Bus merchants who handle bookings on behalf of other merchants may also be allowed to facilitate authentication on behalf of these merchants' Acquirers. When doing so they are operating as a travel agent and so should populate the 3DS message accordingly.

Additional Principles for Travel Use Cases	Rationale
8. Any Travel Agent wishing to facilitate authentication on behalf of other travel merchants' Acquirers must use 3DS version 2.1 or later	To facilitate authentication on behalf of other merchants' Acquirers, the agent must use 3DS/ 3RI functionality which is only possible with the use of 3DS 2.1 or later version.[1] Where the Issuer is not supporting 3DS 2.1 or above, the 3DS 3RI functionality will not be available. In such a situation only one CAVV can be obtained by the Agent for use by one single merchant. The direct to authorization flow for exemptions (as described in Section 4.2.5 of the *PSD2 SCA for Remote Electronic Transactions Implementation Guide*.) should not be used when facilitating authentication on behalf of other merchants' Acquirers, because if the exemption is rejected at time of authorization by the PSP, the cardholder may no longer be available to be authenticated.
9. Issuer must respond to a 3RI Request with no challenge	All Issuers who support 3DS 2.1 and above must respond to a 3RI request. No challenge will be possible as the cardholder is not available when 3RI is used.
10. Determining the amount to be authenticated at booking	At booking, the merchant should authenticate for the maximum amount that the customer can be charged without the need for further cardholder interaction/authentication. • If a full or partial amount is being paid upfront (e.g. purchasing airline tickets) then no further interaction will be required so the amount to be paid upfront should be authenticated. • No Show and prepayment amounts that may be processed later but prior to further interaction with the cardholder should not be authenticated as they will be processed as MITs. • For all amounts to be charged only after a further cardholder interaction takes place (e.g. hotel check in, car rental pick up), no authentication is required for those amounts as they can be handled directly by the merchant either in face-to-face or in their mobile app. If the booking is made via an Agent, the Agent is not likely to know what the merchant will charge and when. Therefore the Agent should authenticate for the total amount of the booking. The Agent should communicate to the cardholder prior to authentication that they are being authenticated for a maximum amount (which must be specified) and that no charges will appear on their card statement until the order is finalized by each merchant according to the specific T&Cs for each part of the booking.

[1] Best practice is to use EMV 3DS 2.2 or later

Additional Principles for Travel Use Cases	Rationale
11. It is the merchant collecting the funds that must process the authorization	It is the name of the merchant collecting the funds that must be populated in the authorization request. If the Travel Agent is not collecting any funds, then it should not authorize and its name should not appear in the authorization request. The Agent can process an Account Verification to check the card is valid.
12. In most cases there is no fraud-related dispute liability protection for MITs	Fraud-related dispute protection for MITs are as follows: • For No Show and Delayed Charges: no fraud-related dispute liability protection applies. As such, a CAVV should not be populated in these transactions. • For incremental MITs: ○ fraud-related dispute liability protection only applies when the MIT is processed subsequent to a card present CIT. ○ When subsequent to a card absent transaction, no fraud-related dispute liability protection applies and therefore a CAVV is not needed. • For re-authorizations (MRC 3903), if a CAVV is populated in the re-authorization fraud-related dispute, liability protection can apply in some cases (see scenarios in section 3 for specific examples).
13. Token Authentication Verification Value (TAVV) based on Cloud Token Framework (CTF) can be used by qualifying token requestors for cardholder authentication	In some cases qualifying token requestors can use the CTF TAVV as evidence of cardholder authentication. In such cases, a CAVV is not required for SCA compliance. CTF TAVVs used in this way do not currently qualify the merchant for fraud-related dispute liability protection. More information will be provided by the Visa Token Service as these new options become available.
14. Token transactions require a TAVV unless they are being submitted as MIT	Visa requires a TAVV (existing or new CTF TAVV) to be present in all Token transactions unless the transaction is identified as an MIT.

3. Payment scenarios and guidance for merchants & PSPs in the Travel & Hospitality Industry

The following subsections provide merchants and Acquirers with examples of how to perform SCA across common Travel and Hospitality payment scenarios, including MITs. The following is provided for each payment scenario:

- A brief description introducing the payment scenario and when it is applicable, *and*
- A step-by-step description of the actions that a merchant should take after each significant event (e.g. order is placed, shipment is made, etc.) occurs. The action taken by the merchant in each step is ***highlighted*** in bold and italics.

The approach for handling each of these scenarios serves only as a recommendation, therefore, merchants and Acquirers can choose alternative options that complement their business model, as long as they remain compliant with the key principles summarised in Section 4.2 of the PSD2 SCA for Remote Electronic Transactions Implementation Guide and Section 2 above.

It is advisable that Issuers also familiarise themselves with the illustrated approach for handling each of the different scenarios, so that they can adopt appropriate authorization policies to minimise unnecessary friction with their customers.

IMPORTANT NOTE:

The main focus of the scenarios presented in this section are merchants providing SCA for PANs and Tokens using 3-D Secure.

In some cases qualifying token requestors can use the Cloud Token Framework (CTF) TAVV as evidence of cardholder authentication. In such cases a CAVV is not required for SCA compliance. TAVVs used in this way do not currently qualify the merchant for fraud-related dispute liability protection. More information will be provided about the Visa Token Service as these new options become available.

3.1 Authentication performed by a Travel Agent on behalf of one single merchant

When a travel booking is made via a Travel Agent, the end merchant(s) (airline, train operator, hotel or car rental agency etc.) do not have an interaction with the cardholder. Therefore if the end merchant(s) will need to process any remote electronic payments prior to their own interaction with the cardholder, they can have an arrangement with the Travel Agent to perform authentication for those payments on behalf of the end merchant's Acquirer.

When the Travel Agent is facilitating authentication on behalf of a single merchant's Acquirer at the time of booking (e.g. the booking involves only one merchant or it involves several merchants, but only one merchant's Acquirer needs authentication to be performed on its behalf), the process is as follows:

Scenario Steps
Customer places an order
1. The Travel Agent discloses to the cardholder appropriate T&Cs and follows other requirements associated with the potential future MIT type the merchant may have to process. The customer must explicitly accept the T&Cs for the agreement to proceed. The merchant should discuss with their Acquirers to ensure they are familiar with the rules associated with their MIT types. For more information, see the Stored Credential Framework and Merchant Initiated Transaction Framework appendices in the *PSD2 SCA for Remote Electronic Transactions Implementation Guide*
Customer authentication
2. The Travel Agent ***authenticates*** the transaction for the total booking amount (see Principle 10 in Section 2). The 3DS authentication request must contain the following information: • Total booking amount • Merchant descriptor name = "Travel Agent Name * name of merchant " • 3DS requestor ID (assigned by Visa) = Agent name (only) Exemptions can be used (subject to Principle 5 in Section 2) if the merchant does not need to process MITs prior to a further interaction with the cardholder (see Principle 6 in Section 2). The CAVV returned and associated ECI value will include the 3DS Requestor ID. Successful authentications will have an associated ECI of 5 unless an exemption was used. When facilitating authentication on behalf of the Acquirer of other merchants, before the authentication step the Travel Agent must clearly communicate the following to the customer: • they are being authenticated for a maximum amount (which must be specified) • no charges will appear on their card statement until the order is finalized by each merchant • the merchant name 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 with each of the separate bookings (e.g. hotel, airline and card rental) Note: When processing a transaction with tokens, qualifying token requestors can provide the merchants with a CTF TAVV as evidence of cardholder authentication. In such cases a CAVV is not required for SCA compliance
3. The Travel Agent may optionally perform an ***account verification*** to check validity of the card before passing the card details to the merchant or merchant's designated payment processor.

- If an account verification is performed, it must not include the CAVV as this is required by the end merchant in step 5.
- If it is processed with a token it must include the TAVV.

4. The Travel Agent ***passes*** the following information to the merchant or their processor* so they can perform an authorization as described in step 5.a or 5.b.
   a) CAVV and associated ECI value, or
   b) CAVV and associated ECI value & TAVV, if transaction was initiated with a token, or
   c) CTF TAVV and associated ECI value, if transaction was initiated with a token under the Cloud Token Framework

* The information can be passed to the entity processing the payment on behalf of the merchant rather than the merchant itself. For airline merchants, this information is generally passed to the Global Distribution System (GDS). In the case of hotel, car rental, railways/buses or other merchants using the booking services of the agent, this information is generally passed to the merchants or its gateway provider.

When payment is processed immediately

5a) When the authorization is performed immediately after receiving the payload from the Travel Agent, the merchant (or its GDS or gateway provider) must submit the transaction with the following:
- The amount of the transaction in accordance with Principle 13 in Section 4.2 of *PSD2 SCA for Remote Electronic Transactions Implementation Guide*
- The CAVV and associated ECI value received from the Travel Agent, or
- CAVV and associated ECI value & TAVV, if transaction was initiated with a token, or
- CTF TAVV and associated ECI value, if transaction was initiated with a token under the Cloud Token Framework
- The merchant name must be the name of the entity who will receive payment. The merchant name presented must be the name the merchant primarily uses to identify itself to the customer as per Visa Rule #27816. (the agent name must not appear in the authorization unless the agent is also the merchant being paid for a particular transaction)

Exemptions can be used (subject to Principle 5 in Section 2) if the merchant does not need to process MITs prior to a further interaction with the cardholder (see Principle 6 in Section 2).

Note: If the merchant needs to process any other authorization for this cardholder prior to further interaction (e.g. Prepayments or No Show), the merchant needs to store the Transaction ID of the authorization performed in step 5a as the "Initial Transaction ID" for future use in those transactions that will have to be indicated with the appropriate MIT indicator and Initial Transaction ID in accordance with Section 3.7 of *PSD2 SCA for Remote Electronic Transactions Implementation Guide*.

Examples of MITs that could be needed by a merchant receiving a booking via a Travel Agent include:
- For Prepayments prior to check in use the Instalment indicator 'I' in Field 126.13
- For No Show payments; MRC 3904

Note: When processing a transaction with tokens, qualifying token requestors can provide the merchants with CTF TAVV as evidence of cardholder authentication. In such cases a CAVV is not required for SCA compliance

When payment is processed at a later time

5b) When the authorization is performed at a later time (for example because amount is not due immediately) after receiving the payload from the Travel Agent, the authorization must be performed in two steps as follows:

i. A zero value ***account verification*** must be performed within 24 hours with the following:
   - The CAVV and associated ECI value received from the agent, or
   - CAVV and associated ECI value & TAVV, if transaction was initiated with a token, or

- CTF TAVV and associated ECI value, if transaction was initiated with a token under the Cloud Token Framework
- If an exemption was applied in the authentication request then it should also be flagged in the account verification.
- The Transaction ID of this account verification must be stored as initial Transaction ID for use in the future authorization.

ii. An authorization when a payment is due, with the following:

- The amount of the transaction in accordance with Principle 13 in Section 4.2 of *PSD2 SCA for Remote Electronic Transactions Implementation Guide*
- The initial Transaction ID obtained in step 5.b.i and the appropriate MIT indicator, for example:
    - For the first authorization of an amount other than zero – reauthorization MRC 39032. An example of a payment needing to be delayed and processed later in this way could be something like when a snowboard is bought at time of booking but is initially out of stock (for more information refer to delayed shipment scenario in section 5 of the *PSD2 SCA for Remote Electronic Transactions Implementation Guide*)
    - For prepayments prior to check in use the Instalment indicator 'I' in Field 126.13
    - For No Show payments; MRC 3904

Note: When processing a transaction with tokens, qualifying token requestors can provide the merchants with CTF TAVV as evidence of cardholder authentication. In such cases a CAVV is not required for SCA compliance

Initial booking completed – refer to Section 3.8 for steps after check in/pick up of service

[2] Merchants wishing to receive fraud-related dispute liability protection for this payment can choose not to include the CAVV in the account verification of step 5.b.i. but to include it in the reauthorization instead in accordance with Principle 12 in Section 4.2 of *PSD2 SCA for Remote Electronic Transactions Implementation Guide*

3.2 Authentication performed by a Travel Agent on behalf of several other merchants

This scenario covers the case when a customer makes a travel reservation online via a Travel Agent which includes the delivery of services by several other merchants. For example, a booking for flights, a hotel and a car rental.

When a travel booking is made via a Travel Agent, the end merchant(s) (airline, train operator, hotel or car rental agency etc.) do not have an interaction with the cardholder. Therefore if the end merchant(s) will need to process any remote electronic payments prior to their own interaction with the cardholder, they could have an arrangement with the Travel Agent to facilitate authentication for those payments on behalf of these merchants' Acquirers.

This should be done as follows when the Agent must perform authentication for more than one merchant during the same booking:

Scenario Steps
Customer books via an online agent
1. The Travel Agent discloses to the cardholder appropriate T&Cs and follows other requirements associated with the potential future MIT type the merchant may have to process. The customer must explicitly accept the T&Cs for the agreement to proceed. The merchant should discuss with their Acquirers to ensure they are familiar with the rules associated with their MIT types. For more information, see the Stored Credential Framework and Merchant Initiated Transaction Framework appendices in the *PSD2 SCA for Remote Electronic Transactions Implementation Guide*
Customer authentication
2. Travel agent then ***authenticates*** the transaction for the total booking amount (see Principle 10 in Section 2). The 3DS authentication request must contain the following information: • Total booking amount • Merchant descriptor name = "Travel Agent Name" • 3DS requestor ID (assigned by Visa) = Agent name (only) Exemptions can be used (subject to Principle 5 in Section 2) if the merchant does not need to process MITs prior to a further interaction with the cardholder (see Principle 6 in Section 2). The CAVV and associated ECI value will include the 3DS Requestor ID. Successful authentications will have an associated ECI of 5 unless an exemption was used. When facilitating authentication on behalf of other merchants/merchants' Acquirers, before the authentication step the Travel Agent must clearly communicate the following to the customer: • they are being authenticated for a maximum amount (which must be specified) • no charges will appear on their card statement until the order is finalized by each merchant • the merchant name(s) for which authentication is being performed. The merchant name(s) 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 with each of the separate bookings (e.g. hotel, airline and card rental) When processing a transaction with tokens, qualifying token requestors can provide the merchants with a CTF TAVV as evidence of cardholder authentication. In such cases a CAVV is not required for SCA compliance

Providing evidence of authentication to merchants
3. An additional 3DS/***3RI authentication request*** is required to provide CAVVs for each further merchant who will perform an authorization. Each 3RI authentication request must contain: • The amount of the transaction (must be lower or equal to the amount authenticated/ set aside for this merchant and the cumulative amount requested for all merchants cannot exceed the amount authenticated in step 2) • Merchant descriptor name = "Travel Agent Name * name of merchant" (e.g. airline or hotel or card rental) • The 3DS Requestor ID (numeric value assigned by Visa to the Agent) • Transaction information from the initial authentication performed in step 2 (such as ACS Trans ID, timestamp, prior transaction authentication method used etc.) • Exemption indicators if exemptions can be used The CAVV returned by each 3DS/3RI request will: • Include the 3DS requestor ID only • will have an associated ECI 5 for successfully authenticated transactions3 (unless an exemption was used) No active challenge will be invoked by ACS as this is not possible with 3RI.
Note: When processing a transaction with tokens, qualifying token requestors can provide the merchants with CTF TAVV as evidence of cardholder authentication. In such cases a CAVV is not required for SCA compliance
4. The Travel Agent may optionally perform an ***account verification*** to check validity of the card before passing the card details to the merchant or merchant's designated payment processor. • If an account verification is performed, it must not include the CAVV as this is required by the end merchant in step 6. • If it is processed with a token it must include the TAVV
5. The Travel Agent ***passes*** the following information to each merchant or their processor* so they can perform an authorization as described in step 6.a or 6.b. • CAVV and associated ECI value, or • CAVV and associated ECI value & TAVV, if transaction was initiated with a token, or • CTF TAVV and associated ECI value, if transaction was initiated with a token under the Cloud Token Framework * The information can be passed to the entity processing the payment on behalf of the merchant rather than the merchant itself. For airline merchants this information is generally passed to the Global Distribution System (GDS). In the case of hotel, car rental, railways/buses or other merchants using the booking services of the agent, this information is generally passed to the merchant or its gateway provider
Payment processed immediately
6a) When the ***authorization*** is performed immediately after receiving the payload from the Travel Agent, the merchant (or its GDS or gateway provider) must submit the transaction with the following: • The amount of the transaction in accordance with Principle 13 in Section 4.2 of *PSD2 SCA for Remote Electronic Transactions Implementation Guide* • The CAVV and associated ECI value received from the Travel Agent, or • CAVV and associated ECI value & TAVV, if transaction was initiated with a token, or

[3] If a N' or 'R' indicating failure or rejection is obtained, Agent or merchant will have to contact cardholder before an authorization can be processed

- CTF TAVV and associated ECI value, if transaction was initiated with a token under the Cloud Token Framework
- If merchant's Acquirer was eligible for exemption and has chosen to exercise those, the appropriate exemption indicator should be included
- The merchant name must be the name of the entity who will receive payment. The merchant name presented must be the name the merchant primarily uses to identify itself to the customer as per Visa Rule #27816 (the agent name must not appear in the authorization unless the agent is also the merchant being paid for a particular transaction)

Exemptions can be used (subject to Principle 5 in Section 2) if the merchant does not need to process MITs prior to a further interaction with the cardholder (see Principle 6 in Section 2).

Note: If the merchant needs to process any other authorization prior to further interaction with the cardholder (e.g. prepayments or No Show), the merchant needs to store the Transaction ID of this authorization step 5a as the "Initial Transaction ID" for future use in those transactions that will have to be indicated with the appropriate MIT indicator and Initial Transaction ID in accordance with Section 3.7 of *PSD2 SCA for Remote Electronic Transactions Implementation Guide*.
Examples of MITs that could be needed by a merchant receiving a booking via a Travel Agent include:

- For prepayments prior to check in use the Instalment indicator 'I' in Field 126.13
- For No Show payments; MRC 3904

Note: When processing a transaction with tokens, qualifying token requestors can provide the merchants with CTF TAVV as evidence of cardholder authentication. In such cases a CAVV is not required for SCA compliance

Payment processed at a later time

6b) When the authorization is performed at a later time (for example because amount is not due immediately) after receiving the payload from the Travel Agent, the authorization must be performed in two steps as follows:

i. A zero value ***account verification*** must be performed within 24 hours with the following:
- The CAVV and associated ECI value received from the Travel Agent, or
- CAVV and associated ECI value & TAVV, if transaction was initiated with a token, or
- CTF TAVV and associated ECI value, if transaction was initiated with a token under the Cloud Token Framework
- If an exemption was applied in the authentication request then it should also be flagged in the account verification

The Transaction ID of this account verification must be stored as initial Transaction ID for use in the future authorization.

ii. An authorization when a payment is due, with the following
- The amount of the transaction in accordance with Principle 13 in Section 4.2 of *PSD2 SCA for Remote Electronic Transactions Implementation Guide*
- The initial Transaction ID obtained in step 5.b.i and the appropriate MIT indicator, for example:
  - For the first authorization of an amount other than zero – reauthorization MRC 3903[4]. An example of a payment needing to be delayed and processed later in this way could be something like when a snowboard is bought at time of booking but is initially out of stock (For more information refer to delayed shipment scenario in section 5 of the *PSD2 SCA for Remote Electronic Transactions Implementation Guide*)
  - For Prepayments prior to check in use the Instalment indicator 'I' in Field 126.13
  - For No Show payments; MRC 3904

[4] Merchants wishing to receive fraud-related dispute liability protection for this payment can choose not to include the CAVV in the account verification of step 5.b.i. but to include it in the reauthorization instead in accordance with Principle 12 in Section 4.2 of *PSD2 SCA for Remote Electronic Transactions Implementation Guide*

Note: When processing a transaction with tokens, qualifying token requestors can provide the merchants with CTF TAVV as evidence of cardholder authentication. In such cases a CAVV is not required for SCA compliance

Initial Booking completed – refer to other scenarios for steps after check in/pick up of service

3.3 Authentication performed by a Travel Agent for itself when acting as a merchant

When a Travel Agent needs to collect funds from the cardholder directly and process an authorization under its own name, the Travel Agent is acting as the merchant and must proceed accordingly. For example, this would be the case if the Travel Agent is selling some of its own services or some promotional items it has pre-purchased from other merchants (such as rooms that have been prepaid and are being resold by the Travel Agent).

In this scenario, the Travel Agent may be able to benefit from authentication exemptions if its Acquirer applies and qualifies for it.

When authenticating for itself only (no authentication required for other merchants during this booking), the process to be followed is the one indicated in *Section 3.1 Authentication performed by a Travel Agent on behalf of one single merchant* except that:

- If using 3DS authentication during step 2: the name of the merchant in the 3DS request must be the "Name of the Agent" only (or the name it uses when acting as a merchant if it differs)
- Step 3 and 4 are skipped

When authenticating also for other merchants during the booking, the process to be followed is the one indicated in *Section 3.2 Authentication performed by a Travel Agent on behalf of several other merchants* except that:

- If using 3DS authentication, in step 3, the Travel Agent must request a separate CAVV for itself via 3RI with
    - the name : Name when acting as a merchant if same as Travel Agent name If not: "Travel Agent Name * name of merchant"
    - The amount allocated to the Travel Agent acting as a merchant
- Steps 4 and 5 can be skipped
- Step 6a or 6.b are performed by the Travel Agent acting as a merchant

3.4 Customer purchases a transport ticket (airline, train, bus, ferry - single company)

The customer purchases a ticket online that is to be charged following completion of booking.

If the purchase is conducted directly on the merchant's website (the merchant providing the service and collecting the payment), this is to be processed as a regular one-time purchase as described in Section 5.1 of the *PSD2 SCA for Remote Electronic Transactions Implementation Guide*. For airline tickets, the additional data requirement needed in clearing for an airline ticket apply as usual.

If the purchase is conducted via an agent, the agent would need to perform authentication on behalf of the transport merchant's Acquirer, unless the Agent is aware the merchant's Acquirer can benefit from a specific exemption and has a request from the Acquirer to authenticate requesting this exemption on its behalf (see Principle 5 in Section 2). Merchants must be aware that if the exemption is declined by the Issuer at time of authorization, the cardholder will no longer be available to be authenticated so exemptions should be used with care.

To perform authentication on behalf of the transport merchant's Acquirer, the Travel Agent must follow the process outlined in Section 3.1 *Authentication performed by a Travel Agent on behalf of one single merchant* above and the merchant (or its GDS for airline or gateway provider for as applicable) will have to perform the authorization as outlined in the same section. Clearing is not impacted and should be performed as usual.

3.5 Customer purchases transport tickets (multiple segments and/or companies / airlines)

The customer purchases multiple transport tickets during a single booking. Tickets are to be charged following completion of booking.

If the purchase is conducted directly on one merchant's website and covers tickets only from that merchant (or provisioned by it – i.e. the merchant is providing the service and collecting the payment), this is to be processed as a regular online purchase with one single authorization as described in Section 5.1 of the *PSD2 SCA for Remote Electronic Transactions Implementation Guide*. For airline tickets, this may be processed with one single authorization but multiple clearing, one for each flight. This is recommended as this requires only one CAVV as described in Section 5.3.1 of the *PSD2 SCA for Remote Electronic Transactions Implementation Guide*. The additional data requirement needed in clearing of an airline ticket applies as usual.

If the purchase is conducted via an agent, the agent will need to perform authentication on behalf of each of the merchants' Acquirers involved in the booking. If the Agent is aware that one of the merchant's Acquirers can benefit from a specific exemption and has a request from this Acquirer to authenticate requesting this exemption (see Principle 5 in Section 2), the Agent could use the applicable exemption for the relevant merchant only. Merchants must be aware that if the exemption is declined by the Issuer at time of authorization, the cardholder will no longer be available to be authenticated so exemptions should be used with care.

If the purchase is conducted by an agent on behalf of a merchant or merchants' Acquirers, the Agent will need to perform authentication on behalf of each merchant's Acquirer that requires it following the processes outlined in either *Section 3.1 Authentication performed by a Travel Agent on behalf of one single merchant* or *Section 3.2 Authentication performed by a Travel Agent on behalf of several other merchants* above and each of the merchant (or its GDS or gateway provider most likely) will have to perform the authorization as outlined in the same sections. If one airline has multiple tickets, it may process one single authorization but multiple clearings, one for each flight, as described in Section 5.3.1 of the *PSD2 SCA for Remote Electronic Transactions Implementation Guide*. Clearing is not impacted and should be performed as usual.

3.6 Customer makes a hotel or car rental reservation (no payment due at reservation)

The customer reserves a hotel or car rental online but no payment is due until check-in / pick-up. In this case no authentication nor authorization is needed, unless the merchant wishes to be in the position to process a "No Show" transaction in accordance with its cancellation policy if the customer does not cancel on time and does not come to honour the reservation.

If the merchant wishes to be able to process a "No Show" in accordance with Visa Rules, it must ensure it puts in place an agreement to later process this No Show, as described in Section 5.9 of the *PSD2 SCA for Remote Electronic Transactions Implementation Guide*.

If the booking is processed by an Agent, the Agent needs to know whether the merchant wishes to be able to process a No Show and if yes, set up the agreement on the merchant's behalf by performing the authentication on behalf of the merchant's Acquirer, for a zero value amount (no amount due that day), as indicated in either *Section 3.1 Authentication performed by a Travel Agent on behalf of one single merchant* or *Section 3.2 Authentication performed by a Travel Agent on behalf of several other merchants* above.

3.7 Customer makes a hotel/cruise or car rental reservation (prepayment or partial payment due at reservation)

The customer reserves a hotel/cruise or car rental online and a prepayment or partial prepayment is due at booking. In this case authentication and authorization must be performed for the amount due on booking.

If this is booked on the merchant website, this is to be processed as a regular one-time purchase as described in Section 5.1 of the *PSD2 SCA for Remote Electronic Transactions Implementation Guide*.

If the merchant also wishes to be in a position to charge for (a) balance payment(s) prior to future interaction with the cardholder, it must ensure it puts in place an agreement with the customer to later process these as follows:

Scenario Steps
Customer confirms booking and pays for what is due today and agrees to additional payment(s) as needed
1. The merchant ***authenticates*** the transaction immediately for the amount due that day, obtaining a CAVV for later submission in the authorization. Applicable exemptions can be exercised which may result in this step being skipped, see Section 4.2.5 of the *PSD2 SCA for Remote Electronic Transactions Implementation Guide*. However, the merchant must be aware that if authentication is required for setting up the agreement for additional prepayment, exemptions should not be used (see Principle 6 in Section 2). The merchant must follow all applicable Visa rules for prepayments including disclosure requirements. Note: When processing a transaction with tokens, qualifying token requestors can provide the merchants with CTF TAVV as evidence of cardholder authentication. In such cases, a CAVV is not required for SCA compliance
2. The merchant performs an ***authorization*** for the full amount due that day with: • CAVV and associated ECI value or • CAVV & TAVV and associated ECI value if transaction was initiated with a token, or • CAVV and associated ECI value & TAVV, if transaction was initiated with a token, or • CTF TAVV and associated ECI value, if transaction was initiated with a token under the Cloud Token Framework The Transaction ID of this authorization must be stored for usage in additional partial prepayments. The receipt for this transaction must fulfil all obligations for both the agreement and the purchase. The merchant must follow all applicable Visa rules for prepayments.
Customer must pay a partial prepayment prior to check-in/pick up

• The merchant ***authorizes*** the prepayment as follows:
• For the amount of the prepayment required
• In accordance with the MIT framework as described in Section 3.7 of the *PSD2 SCA for Remote Electronic Transactions Implementation Guide*
  ○ With the transaction ID obtained at step 2
  ○ For prepayments prior to check in use the Instalment indicator 'I' in Field 126.13
• No CAVV or TAVV required as this is an MIT

Customer checks-in

3. Refer to Section 3.8 below.

If the customer does not show and does not cancel per the prescribed cancellation policy, some or all of the prepayment will be forfeited as specified in Visa Rules.

If the booking is handled via a Travel Agent, follow the process indicated in either *Section 3.1 Authentication performed by a Travel Agent on behalf of one single merchant* or *Section 3.2 Authentication performed by a Travel Agent on behalf of several other merchants* above for the amount due at booking. If the Travel Agent must also set up an agreement for (a) balance payment(s) prior to future interaction with the cardholder, it must disclose the appropriate terms of the agreement. The merchant will need to store the Transaction ID of the initial authorization and process the prepayments with appropriate MIT indicators.

3.8 Payments for Hotel Stays, Cruise On-board Charges or Car rental from check-in, embarkation, pick-up to end of stay/rental

There are two ways to perform these payments:

3.8.1 Option 1 – with card present check-in/embarkation/pick-up at the reception counter

Scenario Steps
Customer checks- in, embarks or picks up the service at reception counter or kiosk
1. An ***authorization*** must be performed at check-in/embarkation/pick-up in order to process the final transaction amount at the end of the stay/rental (if this was not prepaid) and/or any incidental charges. This transaction is a face-to-face CIT and SCA is required: • SCA requirements must be met (e.g. chip and PIN) and the merchant must inform the cardholder that further charges may apply (e.g. via T&Cs) • An estimated amount should be used (using estimated indicators – no incremental transaction can be processed unless preceded by an estimated authorization) • No exemption should be used as this CIT is also used to set up the agreement to process incremental and delayed charges which are MITs (see Principle 6 in Section 2). • The transaction ID of this CIT must be stored for usage in the processing of any MITs (incremental or delayed charges) during or after completion of the stay / rental period without being asked for authentication
Customer incurs additional charges during stay or rental
2. If an estimated amount was processed at check-in/embarkation pick-up, the merchant can ***authorize*** additional charges as MITs. However, for an MIT to receive authorization without the Issuer asking for authentication, the transaction must be properly indicated using the MIT framework: • The merchant processes a transaction for the additional amount using the Incremental MRC 3900 and the Initial Tran ID obtained in step 1 • This step may be repeated as many times as needed during the stay
Stay or service completed (e.g. checkout, return car)

3. The process for check out varies depending on whether the checkout is remote or face to face.
If an express checkout is used without the cardholder being present and the merchant has clearly explained and obtained agreement to an 'express checkout' when the initial authorization occurred, the following applies (this assumes that the total amount charged remains within the cardholder's reasonable expectations and within the scope of its initial agreement with the merchant, if not, a new authentication is required):
   - If final transaction amount is lower than the authorized amount but within a 15% variance of the total cumulative authorized amount
     - Merchant ***clears*** the transaction for the final amount. No further authorization needed
   - If final amount is within a 15% variance of the total cumulative authorized amount
     - Merchant ***clears*** the transaction for the final amount. No further authorization needed
   - If final amount is higher than 15% of total cumulative authorized amount
     - Merchant must do one last ***Incremental authorization*** for additional/not yet authorized amount, using MIT Incremental indicator and initial Transaction ID from step 1.
     - Merchant then ***clears*** the transaction for final cumulative authorized amount
   - If final transaction amount is more than 15% lower than the total cumulative authorized amount, a partial ***reversal*** must be processed for excess authorization amount. Then the merchant ***clears*** the transaction for the final amount.

   If a checkout is completed face-to-face:
   - The process is exactly as above except that final amount can be completed as a card present transaction (e.g. Chip and PIN)

Additional charges occur after check-out/return

4. If a merchant must charge for any incidental charges after checkout/return, the transaction must be processed as a Delayed Charges MIT using the MRC 3902 and the Transaction ID from step 1.

Booking fully closed

Note that if a merchant is unable to support the MIT framework, it can only authorize a known amount at check-in with chip and PIN and then perform a further authentication and authorization each time new charges are accrued. To do this, the merchant will need to ask the cardholder to come to perform a card present transaction (e.g. Chip and PIN) for another known amount at reception or a kiosk.

3.8.2 Option 2 – check in via the merchant's mobile app

In cases where the merchant provides the cardholder with a mobile app to perform check-in and possibly enable a key, the following applies.

Note that when the cardholder will be providing its account details for the first time for storage by the merchant app, the stored credential framework must be followed. This means that Visa needs to receive an authorization request with the value "C" in field 126.13. This can be done prior to check in during a zero value authorization or during the authorization listed in step 1 below.

Scenario Steps
Customer checks-in or picks up the service via mobile app
1. An authorization must be performed at check-in/embarkation/pick up in order to process the final transaction amount at the end of the stay/rental (if this was not prepaid) and/or any incidental charges. As it is performed via a mobile app using a stored credential, this transaction is an eCommerce CIT and SCA is required if any MITs are to be subsequently processed for additional charges. Therefore, the first step required is that the merchant must ***authenticate*** for the initial estimated amount and inform cardholder that further charges may apply (e.g. via T&Cs). No exemption should be used as this CIT is also used to set up future MITs (see Principle 6 in Section 2).
2. ***Authorization*** must be processed for an estimated amount (using estimated indicators – no incremental transaction can be processed unless preceded by an estimated authorization). The authorization must include either: a. CAVV and associated ECI value, or b. CAVV and associated ECI value & TAVV, if transaction was initiated with a token, or c. CTF TAVV and associated ECI value, if transaction was initiated with a token under the Cloud Token Framework The transaction ID of this CIT must be stored for usage in the processing of any MITs (incremental or delayed charges) during or after completion of the stay /rental period without being asked for authentication.
Customer incurs additional charges during stay or rental
3. The merchant must ***authorize*** subsequent additional charges identified as Incremental MITs. To receive authorization without the Issuer asking for authentication, the transaction must be properly indicated using the MIT framework: • The merchant authorizes for the additional amount using the Incremental MRC 3900 and the Initial Transaction ID obtained in step 1 • This step may be repeated as many times as needed during the stay • As the transaction is an MIT, no CAVV or TAVV is required
Stay or service completed (e.g. checkout, return car)
4. If an express checkout is used without cardholder present and the merchant has clearly explained and obtained agreement to an 'express checkout' when the initial authorization occurred, the following applies (this assumes that the total amount charged remains within the cardholder's reasonable expectations and within the scope of its initial agreement with the merchant – if not, then a new authentication is required): • If final transaction amount is lower than the authorized amount but within a 15% variance of the total cumulative authorized amount

- Merchant ***clears*** the transaction for the final amount. No further authorization needed
- If final amount is within a 15% variance of the total cumulative authorized amount
  - Merchant ***clears*** the transaction for the final amount. No further authorization needed
- If final amount is higher than 15% of total cumulative authorized amount
  - Merchant must do one last ***Incremental authorization*** for additional/not yet authorized amount, using MIT Incremental indicator and initial Transaction ID from step 1
  - Merchant then ***clears*** the transactions for final cumulative authorized amount
- If final transaction amount is more than 15% lower than the total cumulative authorized amount, a partial ***reversal*** must be processed for excess authorization amount. Then the merchant ***clears*** the transaction for the final amount.

Additional charges occur after completion

5. If a merchant must charge for any incidental charges after checkout/return the ***authorization*** must be processed as a Delayed Charges MIT using the MRC 3902 and the Transaction ID from step 1.

Booking fully closed