AMERICAN EXPRESS

PSD2 Guide - Including Travel
October 2020

This document should be used with the Global Credit Authorization Guide (GCAG), ISO and XML formats.

DON'T *do business* WITHOUT IT™

Summary of Changes Table

The Summary of Changes (SOC) is a broad overview of technical changes made to the specification since its last publication. This information may affect the way a Merchant, Third Party Processor or Vendor processes American Express Card transactions. Other changes, including but not limited to, clarification, formatting and consistency updates are included in the Revision Log located at the back of this specification. Changes documented in the SOC are indicated with a revision mark within the specification. Changes that affect multiple locations may or may not be indicated with a revision mark. A trash bin icon identifies where content was removed.

DATA FIELD / SECTION	WHAT CHANGED	WHY THE CHANGE
Cover Page and Header		
	Changed the Cover page and header information to 'PSD2 Guide - Including Travel' (no revision marks for this entry).	Update
Section 1.3 Document Changes		
	Updated to align with new document title.	Update
Section 3.5 Unattended Terminals for Transport Fares and Parking Fees		
	For MCC Codes 7523 and 4784, in the POSDC4 column, added 'Z'.	Update
Section 4.2 SCA Requirements in a Remote Environment		
	For SCA Required, changed bullet to 'Electronic commerce (POS DC 4 or 5, value "S") bearing the SafeKey cryptogram provided during the authentication process'.	Update
Section 5.4 Corporate Exemption		
	In the first paragraph, changed the last sentence to 'These are often referred to as "lodged cards" and typically are Business to Business relationships. Examples include but are not limited to: Travel Management Companies and Corporate Buyer / Supplier Relationships'.	Updates
	Reworded the last paragraph.	
Section 5.5 Credential on File		
	Updated section.	Update
Section 6.2 Transaction ID and Original Transaction ID		
	In the first paragraph, changed the last sentence to 'For additional information, refer to the Global Credit Authorization Guide., ISO and XML formats'.	Update
Section 6.3.5 Reauthorisation		
	Changed the second sentence to 'Common instances that require reauthorisations include delayed shipments, split shipments, extended stays, extended rentals and debt recovery'.	Update
Section 6.4 MIT Transactions and Authorisation Specification Changes		
	Reworded the second paragraph.	Update

Summary of Changes Table (continued)

DATA FIELD / SECTION	WHAT CHANGED	WHY THE CHANGE
Section 7.0 High Level Transaction Types and POS Data Code Values		
	In the first table, changed 'Digital Wallet' to 'Digital Wallet - In App'.	Updates
	Moved Digital Wallet to the third table.	
Section 7.2 High Level Transaction Types and POS Data Code Values		
	In the first table, changed 'Digital Wallet' to 'Digital Wallet - In App'.	Updates
	Moved Digital Wallet to the third table.	
	In the Merchant-Initiated Transaction - Credential on File table, added the following and highlighted the applicable values 'Note: If not supporting DF113, American Express will on an interim basis accept the fields highlighted as MIT. Please note that if no OTID is present the CIT and MIT must have the same MID for authorisation'.	
Section 7.3 Use Cases and POS Data Code Guidance - Online Payments		
	Changed the description for Dynamic Linking to 'Transactions for which the final amount is unknown: UK Finance have published guidance for **UK issued cards** only confirming that a tolerance between authentication and authorisation is acceptable if within the payer's reasonable expectations. The % tolerance will be aligned with the current American Express Estimated Charge Policy. Please note: This approach still requires FCA approval. **EEA issued cards** (excluding UK) cannot benefit from any tolerance'.	Updates
	For Case #28 Third Party Authentication, merged DF61, DF113, DF60 and DF22 positions.	
	Added Case #29 Transit Automated Debt Recovery.	
Section 9.0 American Express SafeKey Comparison Chart		
	In the American Express SafeKey Comparison Chart, added rows for 'Request challenge (MIT mandate set-up / PSD2 SCA)' and 'Merchant-Initiated authentications - 3DS Requestor Initiated (3RI) payments and Decoupled'.	Update
Section 10.0 Indirect Travel Booking Sales		
	Added section.	New section added
Section 11.0 Countries Subject to SCA		
	Added section.	New section added

Table of Contents

Table of Contents

1.0 About the Revised Payment Services Directive

The revised Payment Services Directive (PSD2) places strong emphasis on Cardmember authentication through the introduction of Strong Customer Authentication (SCA). The regulator has agreed to a managed roll out of the SCA requirements for electronic commerce transactions. It is understood though that the whole payment ecosystem should strive to apply SCA in all European Economic Area (EEA) member states as soon as possible.

Disclaimer: This information is for guidance purposes only and should not be regarded as a substitute for taking legal advice. You are encouraged to seek the advice of a competent professional where you require clarification on laws and regulations. To the maximum extent permitted by law, American Express does not make and hereby disclaims any and all representations, warranties, and liabilities, whether express or implied, or arising by law or from a course of dealing or usage of trade, including implied warranties of merchantability or fitness for a particular purpose or any warranty of title or non-infringement. You must comply with laws and regulations applicable to the subject matter of this document. These laws and regulations can differ from country to country, and you are solely responsible for being aware and adhering to them in all countries where you implement this document.

The document must be read alongside the *Global Credit Authorization Guide (GCAG),* ISO and XML formats, and outlines the technical requirements to support PSD2. See Section 7.0 Technical Reference.

1.1 Who Should Use this Document

This document is designed to provide Merchants, authorised Third Party Processors, software vendors and third party programmers with the necessary guidance to support compliance with PSD2.

1.2 Contact Information

To notify us when content clarifications are required, send an email to SpecQuestions@aexp.com, or contact your American Express representative.

1.3 Document Changes

Changes to the *PSD2Guide - Including Travel* are identified in various ways.

Summary of Changes Table — The *PSD2Guide - Including Travel* begins with a Summary of Changes (SOC) table that provides a broad overview of technical and/or data field changes since the last publication. The summary includes the following:

- The data field or section where revision occurred
- A brief description of the revision
- Reason for the change

Changes in the SOC table will be indicated by a revision mark.

1.3 Document Changes (continued)

Revision Mark — Throughout this document, revised areas that may affect the way a Merchant, Third Party Processor or Vendor processes transactions are indicated with a revision mark. This mark is a blue line that appears in the page margin, next to where a change was made. The revision mark is used for content additions and changes. See example of a revision mark at left.

Trash Bin — The following symbol is used to indicate removed text. This symbol appears to the left near the area where text was removed.

Revision Log — The Revision Log is the last section in this document, and it contains a condensed overview of changes made in the last three publications. Changes in the Revision Log may or may not be indicated with a revision mark.

1.4 Related Documents

- *American Express Global Credit Authorization Guide,* ISO Format
- *American Express Global Credit Authorization Guide,* XML Format
- *Notification of Specification Changes (NOSC),* October 2019
- *EMV® 3-D Secure Protocol and Core Functions Specifications v2.X* (this document is issued and owned by EMVCo (www.emvco.com)
- *American Express 2.0 Protocol specification version 2.10* (www.americanexpress.com/merchantspecs)
- *American Express SafeKey 2.0 Acquirer-Merchant Implementation Guide* (www.americanexpress.com/merchantspecs)

EMV® is a registered trademark in the U.S. and other countries and an unregistered trademark elsewhere. The EMV trademark is owned by EMVCo, LLC.

2.0 Strong Customer Authentication Requirements

SCA obliges payment service providers, like American Express, to confirm that the person carrying out certain actions, including initiating an electronic payment transaction, is in fact the legitimate Cardmember. SCA is intended to improve the security of electronic payment transactions, reduce electronic payment fraud and increase customer confidence.

SCA must be applied whenever the Cardmember accesses their payment account online, initiates an electronic payment transaction or carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

SCA requirements are based on "two-factor authentication", meaning that when the SCA obligation is triggered, the verification process must include at least two of the following three authentication elements:

- knowledge (something only the user knows)
- possession (something only the user possesses)
- inherence (something the user is)

Only one element from each category should be used. The authentication elements must be mutually independent so that the breach of one element does not compromise the reliability of the others. The authentication elements must be designed in such a way as to protect the confidentiality and integrity of the Cardmember's personal security details.

These requirements will apply to all electronic transactions made using a card issued in the EEA and affect both card present (e.g. at a point of sale within the EEA) and card not present environments.

Further, for electronic remote payment transactions (e.g. online purchases), there is an additional requirement on American Express to ensure that the above SCA elements dynamically link the transaction to a specific amount and payee.

There are exemptions from SCA for certain transactions such as the 'Transaction Risk Analysis' (TRA) exemption, trusted beneficiary exemption (also known as whitelisting or Express List for American Express) and the Corporate Exemption. There are also certain transactions that are out of scope from these SCA requirements, such as Merchant-Initiated Transactions (MIT) and Mail or Telephone Order (MOTO) Transactions. These are explained further below.

American Express is committed to complying with these requirements in both card present and remote environments. This present guide aims to provide clarity to American Express Merchants around the scope of SCA, its exceptions and exemptions as understood by American Express.

American Express will continue to monitor the regulatory environment and may issue changes to this document as and when it receives further updates or guidance from local regulators.

this page intentionally left blank

3.0 Changes to Transactions Made at Point of Sale

3.1 Chip and PIN

Except where the contactless or unattended terminals for parking and transport exemptions (each described below) apply, all point of sale (in person) transactions must be carried out using the card chip and Personal Identification Number (PIN). Cardmembers must dip (insert) their cards in the terminal and enter their PIN.

American Express will continue to accept chip and signature transactions where we are able to apply a two-factor authentication. If this is not possible, the transaction will be declined as we will be unable to meet the SCA regulation requirements.

3.2 Contactless Exemption

Where the customer is initiating a contactless payment transaction, the application of SCA through use of Chip and PIN will not be required if the following two conditions are met:

- the individual amount of the contactless transaction does not exceed EUR 50 (or local currency equivalent; and
- the cumulative amount of previous contactless transactions initiated using the card since the last application of SCA does not exceed EUR 150 (or local currency equivalent); or the number of consecutive contactless transactions initiated via that card since the last application of SCA does not exceed five.

American Express has opted for the EUR 150 threshold.

3.3 Credential on File and Industry Practice

Where the cardmember is present at the point of sale with his/her card, Chip and PIN is now the only acceptable authentication method unless the contactless exemption applies.

3.4 Fallback to Magnetic Stripe Mode

Transactions carried out using the magnetic stripe functionality of the card will be declined, with the exception of magstripe only cards (issued outside of the EEA).

3.5 Unattended Terminals for Transport Fares and Parking Fees

SCA will not be required for transactions initiated at unattended terminals for transport fares and parking fees (e.g. train and bus fares, toll fees). Our current understanding of the regulation is that the exemption applies to the following categories:

Transport Exemption		
MCC Code	**MCC Description**	**POSDC4**
4111	Local and Suburban Commuter Passenger Transportation including Ferries	2, 4, 5 or Z
4112	Passenger Railways	2, 4, 5 or Z
4131	Bus Lines	2, 4, 5 or Z
7523	Parking Lots and Garages	2, 4, 5 or Z
4784	Tolls and Bridge Fees	2, 4, 5 or Z

It is important that unattended terminals are flagged as such in the Authorisation message.

3.6 Failure to Apply SCA at Point of Sale

In order to fully comply with the requirements, American Express is deploying a new Action Code which will be sent in the Authorisation Responses where American Express determines that the SCA requirement has not been met. See Section 7.1 1110 Authorisation Response.

Merchants and Third Party Processors must ensure full compliance with this new Action Code so that the point of sale prompts the customer to insert the card into the terminal. For more information or testing, contact your American Express representative.

3.7 Transactional Data Quality

American Express is committed to fully comply with the terms of PSD2 whilst endeavoring to avoid disruptions to the transaction flow. It is essential that the data sent to American Express accurately reflects the transaction type. Failure to achieve this standard will result in transactions being declined.

4.0 New Regulatory Landscape for Remote Transactions and Actions

4.1 What is a Remote Environment?

Remote transactions include all electronic payments made using a card or a digital wallet over the internet. Excluded from this category are face to face payments, including those made using a wallet (these are considered proximity or non-remote payments).

4.2 SCA Requirements in a Remote Environment

In the remote environment, only the following types of transactions will be deemed compliant with the SCA requirement:

SCA Required:

- Electronic commerce (POS DC 4 or 5, value "S") bearing the SafeKey cryptogram provided during the authentication process

Exempt from SCA:

- Remote transactions carried out via a secure corporate process and bearing the Corporate Exemption indicator in Data Field 113

Out of Scope:

- Remote transactions flagged as MIT using the relevant subfield of Data Field 113
- Transactions via Mail Order or Telephone Order and flagged as such in the POS Data Code 5 (respectively values 2 and 3)

American Express SafeKey® (EMV 3-D Secure 1.0 or preferably EMV 3-D Secure 2.X) is the approved solution to meet the SCA requirements in the remote environment, however for Credential on file (see Section 5.5 Credential on File) and MIT Mandate (see Section 6.1 MIT Mandate/Pre-Authorisation) you must use EMV 3-D Secure 2.X. Contact your local American Express representative who will advise on the steps required to enroll in American Express SafeKey.

4.3 Failure to Satisfy SCA Requirements in a Remote Environment: New Action Code

In order to fully comply with the regulation, American Express is deploying a new Action Code which will be sent in the Authorisation Response when the remote SCA requirement has not been met.

See Section 7.1 1110 Authorisation Response.

Merchants and Third Party Processors must ensure full compliance with this new Action Code.

For more information or testing, contact your American Express representative.

4.4 Mail Order and Telephone Order (MOTO Transactions)

All transactions initiated by mail, e-mail or telephone are currently considered as out of scope of the SCA requirement.

In order to accurately identify transactions as MOTO, American Express relies on **specific values** in Data Field 22, POS Data Code.

Refer to the American Express *Global Credit Authorization Guide* for more information.

For more information or testing, contact your American Express representative.

4.5 Transactions Submitted Prior to 14 September 2019

This concerns the scenario where a transaction is initiated prior to 14 September 2019 and continues after 14 September 2019. For Card Provision / Storage - There is no requirement to apply SCA to cards provisioned / stored prior to 14 September 2019. For MIT Recurring Billing - There is no requirement to apply SCA to a mandate transaction (CIT) authorised prior to 14 September 2019. After this date the subsequent transactions can still be processed as MIT Recurring Billing. For MIT Single Transaction - There is no requirement to apply SCA to an initial mandate transaction (CIT) authorised prior to 14 September 2019. After this date the transaction (e.g. no show fees) can still be processed as an MIT Single Transaction.

5.0 Other Exemptions from Strong Customer Authentication

5.1 Low Value Transactions

American Express' approach is to request the usage of SafeKey for every single transaction. This allows for the fraud liability shift in favour of the Merchant.

Consequently, as Issuer Transaction Risk Analysis (TRA) is in place, American Express would look to green flow as many of these transactions as possible, especially for low value transactions.

At this stage, American Express does not require a low value exemption indicator in the Authorisation message.

5.2 Transaction Risk Analysis

There is an exemption from the requirement to apply SCA in circumstances where the transaction is identified by American Express as posing a low level of risk. In order to determine whether this exemption is applicable, American Express requests the use of SafeKey for every single transaction. This provides American Express with the information it needs to make a determination about the level of risk posed by the transaction, and may also allow the Merchant to benefit from fraud liability shift.

At this stage, American Express does not require a transaction risk analysis exemption indicator in the Authorisation message.

5.3 Trusted Beneficiaries

There is an exemption from the requirement to apply SCA where a payer initiates a transaction and the payee is included in a list of trusted beneficiaries created by the payer. SafeKey Express List is a service that we provide to our Cardmembers, enabling them to populate a list of sellers they frequently shop with. This is commonly referred to as 'whitelisting'. The Express List provides the Cardmember with the capability in the SafeKey journey to select Merchants to exclude from SCA.

If a Cardmember has added a Merchant to their Express List, SCA will not need to be applied. In order to benefit from this exemption, Merchants must send the transaction to SafeKey where the Express List will be held. If the Merchant appears on the Express List, the transaction will then process with no SCA being applied.

5.3 Trusted Beneficiaries (continued)

The decision to add a Merchant to the Express List is between the Cardmember and the Issuer, there is no Merchant or Acquirer involvement. The Fraud liability for Express List transactions sits with the Issuer.

At this stage, American Express does not require a trusted beneficiary indicator in the Authorisation message.

5.4 Corporate Exemption

Finally, there is also an exemption from the requirement to apply SCA to payments initiated through the use of dedicated payment processes or protocols that are only made available to non-consumers, and which our regulators are satisfied provide equivalent levels of security as SCA. These are often referred to as "lodged cards" and typically are Business to Business relationships. Examples include but are not limited to: Travel Management Companies and Corporate Buyer / Supplier Relationships.

American Express intends to fully apply this exemption where possible, to its various corporate payment products. Although American Express can in most instances apply the Corporate Exemption, we have developed a Secure Corporate Payment indicator in our authorisation specifications which can be used by a Merchant to identify an electronic payment transaction that has leveraged a dedicated process or protocol made available to non-consumers, and which the relevant regulator is satisfied gives an equivalent level of security as that afforded by SCA.

American Express will rely on the Secure Corporate Exemption contained within Data Field 113. Refer to Section 8.1 in the *Global Credit Authorization Guide*, ISO and XML formats.

5.5 Credential on File

American Express allows the use of Credential on File for both Customer-Initiated and Merchant-Initiated Transactions.

Under the terms of the PSD2, the process of storing the credential by a Merchant must follow specific SCA requirements:

- SCA must be carried out in all cases as no exemption is allowed.
- The SafeKey authentication process must involve a one time password which the Merchant will request using the appropriate value in the 3DS Requestor challenge indicator. Refer to the *EMV 3-D Secure Protocol and Core Functions Specifications v2.X*.

When the card is being stored at the same time that an MIT mandate is agreed, only one request challenge authentication process will be required.

Merchants are reminded that, under PCI Data Security Standard requirement #3, **it is prohibited from ever storing the CID/CVV/CSC data**. Merchants must also mask or otherwise encrypt PAN if they store such Cardholder data.

For further information, please visit the PCI website at: www.pcisecuritystandards.org.

6.0 Out of Scope Transactions (Merchant-Initiated Transactions)

SCA only applies to payments initiated by the payer. This means that payment transactions that are not initiated by the Cardmember but by the Merchant are not subject to SCA where those transactions are initiated without any interaction or involvement of the payer.

6.1 MIT Mandate / Pre-Authorisation

Where a Cardmember has given a mandate by agreeing to the Terms & Conditions authorising the Merchant to initiate a transaction or a series of transactions, and where the mandate is based on an agreement between the Cardmember and the Merchant for the provision of products or services, the transactions initiated thereafter by the Merchant on the basis of such mandate can be qualified as MIT, provided that these transactions do not need to be preceded by a specific action of the Cardmember to trigger their initiation by the Merchant.

Where this mandate of the Cardmember is provided through a remote channel (i.e., online), the setting up of such a mandate is subject to SCA. Please note that if the mandate is provided through MO or TO channel, no SCA is required.

The MIT mandate cannot benefit from any exemption and therefore requires a One Time Password (OTP). The Merchant must initiate this process by using the relevant value in the 3DS Requestor Challenge Indicator. For more information, refer to the *EMV 3-D Secure Protocol and Core Functions Specifications v2.1.0*.

While subsequent transactions are MIT, when the Cardmember amends the series/arrangements, SCA must be applied accordingly.

MIT transactions may include subscription-based purchases or plans, contractual arrangements such as hotel (e.g. no show fees) and car rental arrangements (e.g. fines for traffic offences, extended hire fees).

6.2 Transaction ID and Original Transaction ID

In addition to the use of the MIT indicators in the Authorisation message as described in this Section 6.2 and Section 7.2 High Level Transaction Types and POS Data Code Values and Section 7.3 Use Cases and POS Data Code Guidance - Online Payments, American Express requires the authoriser to submit the Original Transaction ID (OTID) in each MIT. For additional information, refer to the *Global Credit Authorization Guide.*, ISO and XML formats.

The Original Transaction ID should be the unaltered Transaction ID sent by American Express in response to the original transaction setting up the MIT mandate (see Section 8.0 PSD2 Data Fields in the Global Credit Authorization Guide).

American Express understands that, in some instances, the original transaction setting up the MIT mandate could have taken place long ago, rendering the storage of the Transaction ID difficult or undesirable. In this particular case, the previous MIT transaction ID would be accepted.

6.2 Transaction ID and Original Transaction ID (continued)

For MIT that have their origins in a mandate prior to the 14th of September or in the case where the Merchant is technically unable to provide this information, we recommend the Original Transaction ID to be left blank as an interim solution. In order to avoid future potential disruptions, we strongly recommend undertaking all necessary steps to provide the Original Transaction ID as described above as soon as possible.

6.3 Types of Merchant-Initiated Transactions

The following are types of Merchant-Initiated transactions:

6.3.1 No Show

A 'no show' transaction occurs when you and a Cardmember have an agreement for a purchase, but the Cardmember does not meet the terms of the agreement. No show transactions are typically used in the hospitality sector.

6.3.2 Recurring Payments

A recurring payment (billing) is a Credential on File (COF) transaction. A series of recurring payments consists of multiple transactions that you bill to a Cardmember at fixed, regular intervals not to exceed one year between transactions. The series of recurring payments is the result of an agreement between you and the Cardmember.

The initial transaction in a series will typically require SCA and should not carry the Recurring Billing indicator in the Authorisation message. Subsequent transactions can then carry the indicator to inform American Express that these are MIT transactions.

6.3.3 Delayed Charges

A delayed charge is associated with an agreement between you and the Cardmember for services rendered. Merchants might use delayed charges after providing services such as lodging, travel, or auto rental.

6.3.4 Unscheduled Payment Transaction

An unscheduled payment transaction (i.e., mobile top up) uses stored payment information for a fixed or variable amount that does not occur on a scheduled or regular basis, provided a pre-authority/mandate is in place.

6.3.5 Reauthorisation

A reauthorisation is a purchase made after an original purchase that can reflect a number of specific conditions. Common instances that require reauthorisations include delayed shipments, split shipments, extended stays, extended rentals and debt recovery. The assumption is that the original purchase transaction would have SCA applied or be exempt from SCA. The original transaction details (including cryptogram when present) must be provided.

6.3.6 Resubmission

A resubmission occurs when you cannot obtain a successful authorisation for a Cardmember-initiated purchase. A resubmission is valid only when the original authorisation was declined for insufficient funds and only for a limited number of days after the original purchase. The assumption is that the original purchase transaction would have SCA applied or be exempt from SCA. The original transaction details (including cryptogram when present) must be provided.

6.4 MIT Transactions and Authorisation Specification Changes

The International Organization for Standardization (ISO) has recently announced the introduction of data elements and values to be used to distinctly identify Merchant-Initiated transactions. American Express aims to adopt these in the future.

American Express will rely on the Merchant-Initiated Indicator contained in Data Field 113. Refer to Section 8.0 1100 Authorization Request, Acceptance Environment Data Table, in the *Global Credit Authorization Guide*).

In addition, Merchants are invited to use the "Credential on File" indicator recently deployed in the *Global Credit Authorization Guide*, Data Field 22 POS Data Code, Value A in positions 1 and 7 in order to reflect accurately the point of sale capability and the transaction context.

The Credential on File indicator can now also be used for Customer-Initiated Transactions.

Out of Scope Transactions - MIT

this page intentionally left blank

7.0 Technical Reference

This section must be used with the *Global Credit Authorization Guide* (ISO and XML formats), and outlines the technical requirements to support PSD2.

7.1 1110 Authorisation Response

The following highlights the new Action Code.

Data Field 39	**ACTION CODE**
Length of Field:	3 bytes, fixed length
Field Type:	Numeric
Constant:	None
Field Requirement:	Mandatory
Description:	This data field contains the Action Code, indicating the American Express disposition for this transaction. Valid Action Codes: `000` Approved `001` Approve with ID `002` Partial Approval (Prepaid Cards only) `100` Deny `101` Expired Card / Invalid Expiration Date `106` Exceeded PIN attempts `109` Invalid Merchant `110` Invalid amount `111` Invalid account / Invalid MICR (Travelers Cheque) `115` Requested function not supported `117` Invalid PIN `119` Cardmember not enrolled / not permitted `122` Invalid card security code (a.k.a., CID, 4DBC, 4CSC) `125` Invalid effective date **`130` Additional customer identification required** `181` Format error `183` Invalid currency code `187` Deny - New card issued `189` Deny - Canceled or Closed Merchant/SE `200` Deny - Pick up card `900` Accepted - ATC Synchronization `909` System Malfunction (Cryptographic error) `912` Issuer not available

7.2 High Level Transaction Types and POS Data Code Values

The following table is a reference for Data Field 22, POS Data Code to support PSD2.

Customer-Initiated Transaction (CIT) at Point of Sale - Card Present

Transaction Type	DF 55 (EMV)	DF 22			
		POSDC1	POSDC5	POSDC6	POSDC7
Chip and PIN	Y	5	0	1	5
Contactless	Y	5	0	X	5
Digital Wallet - In App	Y	5	0	Z	5

Customer-Initiated Remote Transaction - No Credential on File

Transaction Type	DF 61 (SafeKey)	DF 113 Position 9 MIT / CIT	DF 22			
			POSDC1	POSDC5	POSDC6	POSDC7
Internet	Y	Initiating Party CIT = 0	1	S	0	1, 6 or S
Mail Order		Initiating Party CIT = 0	1	2	0	1, 6 or S
Telephone Order		Initiating Party CIT = 0	1	3	0	1, 6 or S

Customer-Initiated Remote Transaction - Credential on File

Transaction Type	DF 61 (SafeKey)	DF 113 Position 9 MIT / CIT	DF 22			
			POSDC1	POSDC5	POSDC6	POSDC7
Internet	Y	Initiating Party CIT = 0	A	S	0	A
In-App Wallet	Y	Initiating Party CIT = 0	A	S	0	A
Digital Wallet	Y	Initiating Party CIT = 0	A	S	0	A
Mail Order		Initiating Party CIT = 0	A	2	0	A
Telephone Order		Initiating Party CIT = 0	A	3	0	A

7.2 High Level Transaction Types and POS Data Code Values (continued)

Merchant-Initiated Transaction - Credential on File

Transaction Type	DF 60 (Original TID)	DF 113 Position 9 MIT / CIT	DF 22			
			POSDC1	POSDC5	POSDC6	POSDC7
MIT Single Transaction	Y	Initiating Party MIT = 1	A	1	0	A
MIT Recurring Billing	Y	Initiating Party MIT = 1	A	9	0	A

Note: If not supporting DF 113, American Express will on an interim basis accept the fields highlighted as MIT. Please note that if no OTID is present the CIT and MIT must have the same MID for authorisation.

Secure Corporate Exemption (SCT) - Lodged Cards

Transaction Type	DF 113 MIT / CIT Position 9	DF 113 SCT Subfield 2	DF 22			
			POSDC1	POSDC5	POSDC6	POSDC7
Secure Corporate Exemption	Initiating Party CIT = 0	SCT Claimed = 1	A	S	0	A

7.3 Use Cases and POS Data Code Guidance - Online Payments

Authentication

- **Authentication** is the process or action of verifying the identity of a customer (person).
- **Authorisation** is the process or action of confirming the card is valid and has sufficient funds for a transaction to be submitted.
- If the transaction amount is subject to change, American Express recommends the authentication is processed for the maximum amount by default. If the amount is not subject to change then the purchase amount will be the maximum amount.
- Maximum Amount - This value can be at a Merchant's discretion as long as the customer understands why the authentication amount is greater than the purchase amount (i.e., a Merchant advises the customer they have chosen to add 10% to the authentication amount to allow for shipping costs).
- The authentication amount **must** always be equal to or greater than the authorisation amount (or total authorisation amounts for split transactions).
- Dynamic Linking – Transactions for which the final amount is unknown: UK Finance have published guidance for **UK issued cards** only confirming that a tolerance between authentication and authorisation is acceptable if within the payer's reasonable expectations. The % tolerance will be aligned with the current American Express Estimated Charge Policy. Please note: This approach still requires FCA approval. **EEA issued cards** (excluding UK) cannot benefit from any tolerance.
- The cryptogram validity is indefinite under the PSD2 regulation. However, the cryptogram authentication expiry is currently 90 under the current terms and conditions. With the exception of some specific industries (e.g. car rental), an authorisation is valid for 7 days.

Note: 'A' in POS DC1 & 7 denotes Credential on File (COF)

MIT/CIT SCENARIOS												
Case #	**Type**	**Description**	**Transaction**	**Authentication Amount Only**	**MIT/ CIT**	**DF 61 SafeKey**	**DF 113 Initiating Party/Corp. Exemption**	**DF 60 OTID**	**POS DC1**	**POS DC5**	**POS DC6**	**POS DC7**
1	Online Groceries 1	An online basket that can be amended (add, changes and deletes) prior to pick and pack. An order is fulfilled and substitutes are offered in place of items which may be greater in value.	Basket changes	Maximum amount and re-authentication is required each time the basket exceeds the maximum amount.	CIT	Y	0		1 or A	S	0	1, 6, A or S
			Pick and Pack	Use final authentication cryptogram.	CIT	Y	0		1 or A	S	0	1, 6, A or S

7.3 Use Cases and POS Data Code Guidance - Online Payments (continued)

Note: 'A' in POS DC1 & 7 denotes Credential on File (COF)

MIT/CIT SCENARIOS												
Case #	**Type**	**Description**	**Transaction**	**Authentication Amount Only**	**MIT/ CIT**	**DF 61 SafeKey**	**DF 113 Initiating Party/Corp. Exemption**	**DF 60 OTID**	**POS DC1**	**POS DC5**	**POS DC6**	**POS DC7**
2	Online Groceries 2	An online basket that can be amended (add, changes and deletes) prior to pick and pack. An order is fulfilled and substitutes are offered in place of items which may be greater in value and a pre-authority / mandate is in place.	Basket changes	Basket amount and re-authentication is required each time the basket exceeds the maximum amount.	CIT	Y	0		1 or A	S	0	1, 6, A or S
			Pick and Pack	N/A	MIT		1	Y	A	1	0	A
3	Recurring Transaction-Frequency and Amount Variation	Purchase of goods/services on a recurring basis where the amounts and frequency may vary and a pre-authority/mandate is in place.	Initial	Maximum amount	CIT	Y	0		1 or A	S	0	1, 6, A or S
			Subsequent	N/A	MIT		1	Y	A	9	0	A
4	Recurring Transaction-Amount Variation	Purchase of goods/services on a recurring basis where the amounts may vary and a pre-authority/ mandate is in place (i.e., Mobile phone bills).	Initial	Maximum amount	CIT	Y	0		1 or A	S	0	1, 6, A or S
			Subsequent	N/A	MIT		1	Y	A	9	0	A
5	Recurring Transaction-Frequency Variation	Purchase of goods/services on a recurring basis where the frequency is set by the Customer and a pre-authority/mandate is in place.	Initial	Maximum amount	CIT	Y	0		1 or A	S	0	1, 6, A or S
			Subsequent	N/A	MIT		1	Y	A	9	0	A

7.3 Use Cases and POS Data Code Guidance - Online Payments (continued)

Note: 'A' in POS DC1 & 7 denotes Credential on File (COF)

MIT/CIT SCENARIOS												
Case #	**Type**	**Description**	**Transaction**	**Authentication Amount Only**	**MIT/ CIT**	**DF 61 SafeKey**	**DF 113 Initiating Party/Corp. Exemption**	**DF 60 OTID**	**POS DC1**	**POS DC5**	**POS DC6**	**POS DC7**
6	Subscription-Standard	A pre-agreed mandate for a series of transactions that can vary in frequency and amount, this would include bundled subscriptions as well as single subscriptions.	Initial	Maximum amount	CIT	Y	0		1 or A	S	0	1, 6, A or S
			Subsequent	N/A	MIT		1	Y	A	9	0	A
7	Subscription Free Trial	A pre-agreed mandate for a series of transactions that can vary in frequency and amount, but the initial period is a free trial.	Initial	Zero amount	CIT	Y	0		1 or A	S	0	1, 6, A or S
			Subsequent	N/A	MIT		1	Y	A	9	0	A
8	Subscription and One-Off Purchase Combined	Purchase of goods/services at the same time as a subscription.	Initial	Maximum amount of goods/ services and subscription	CIT	Y	0		1 or A	S	0	1, 6, A or S
			Subsequent	N/A	MIT		1	Y	A	9	0	A
9	Web-based Services	Purchase of web-based services with periodic billing for variable amounts where a pre-authority/mandate is in place and the payment initiation is not dependent upon a specific action of the payer.	Initial	Maximum amount	CIT	Y	0		1 or A	S	0	1, 6, A or S
			Subsequent	N/A	MIT		1	Y	A	9	0	A

7.3 Use Cases and POS Data Code Guidance - Online Payments (continued)

Note: 'A' in POS DC1 & 7 denotes Credential on File (COF)

MIT/CIT SCENARIOS												
Case #	**Type**	**Description**	**Transaction**	**Authentication Amount Only**	**MIT/ CIT**	**DF 61 SafeKey**	**DF 113 Initiating Party/Corp. Exemption**	**DF 60 OTID**	**POS DC1**	**POS DC5**	**POS DC6**	**POS DC7**
10	Online Service Fees	Online services that vary based on usage. For example, advertising services.	Initial	Maximum amount	CIT	Y	0		1 or A	S	0	1, 6, A or S
			Subsequent	N/A	MIT		1	Y	A	9	0	A
11	Automatic Top-Ups	Automatic reload on a periodic schedule or a variable amount based on balance thresholds specified by the customer.	Initial	Maximum amount	CIT	Y	0		1 or A	S	0	1, 6, A or S
			Subsequent	N/A	MIT		1	Y	A	9	0	A
12	Pre-Orders	Purchase of goods/services where there is a time delay between authentication and final authorisation (e.g. items on sale before release).	Single	Maximum amount	CIT	Y	0		1 or A	S	0	1, 6, A or S
13	Try-Before-You-Buy Programs	Purchase of goods/services where there is a time delay between authentication and final authorisation (e.g. Try-Before-You-Buy Programs where a Customer can order goods and only be billed for the items they keep).	Single	Maximum amount	CIT	Y	0		1 or A	S	0	1, 6, A or S
14	Digital Fulfillment	Purchase of digital products where the provider does not process the charge immediately.	Single	Maximum amount at time of purchase	CIT	Y	0		1 or A	S	0	1, 6, A or S

7.3 Use Cases and POS Data Code Guidance - Online Payments (continued)

Note: 'A' in POS DC1 & 7 denotes Credential on File (COF)

MIT/CIT SCENARIOS												
Case #	**Type**	**Description**	**Transaction**	**Authentication Amount Only**	**MIT/ CIT**	**DF 61 SafeKey**	**DF 113 Initiating Party/Corp. Exemption**	**DF 60**	**POS DC1**	**POS DC5**	**POS DC6**	**POS DC7**
15	Shipping Changes	Post-authentication shipping/fulfillment costs/changes calculated.	Single	Maximum amount including estimated shipping costs	CIT	Y	0		1 or A	S	0	1, 6, A or S
16	Voice Orders	Purchase of goods/services via voice technology without the use of telephone (i.e., Alexa, Siri, etc.).	Single	Maximum amount	CIT	Y	0		1 or A	S	0	1, 6, A or S
17	Fast Track Products	Purchases of goods/services via a fast track method (i.e., one click).	Single	Maximum amount	CIT	Y	0		1 or A	S	0	1, 6, A or S
18	In-App	Purchase of goods/services via an 'In- App' solution (i.e., Taxi (adding a card to the app should follow the athen- tication process for that type)).	Single	Maximum amount	CIT	Y	0		1 or A	S	0	1, 6, A or S
19	Adding a Card to a Wallet/ Account	A consumer adds a card to a Merchant's wallet/account for storage.	Single	Zero or nominal amount	CIT	Y	0		1	S	0	1, 6, or S

7.3 Use Cases and POS Data Code Guidance - Online Payments (continued)

Note: 'A' in POS DC1 & 7 denotes Credential on File (COF)

MIT/CIT SCENARIOS												
Case #	**Type**	**Description**	**Transaction**	**Authentication Amount Only**	**MIT/ CIT**	**DF 61 SafeKey**	**DF 113 Initiating Party/Corp. Exemption**	**DF 60 OTID**	**POS DC1**	**POS DC5**	**POS DC6**	**POS DC7**
20	Reservation - Advance Prepayment	A Customer places a reservation and pays for good/services i.e. Hotel room.	Single	Maximum amount	CIT	Y	0		1 or A	S	0	1, 6, A or S
21	Reservation - Advance Deposit	A Customer places a reservation paying a deposit for good/services (i.e., package holiday). Authentication at the time of the reservation will allow for future MIT transactions using the reservation pre-authority/mandate when the Customer is not present.	Single	Maximum amount	CIT	Y	0		1 or A	S	0	1, 6, A or S
22	Reservation - Payment On Site	A Customer places a reservation paying on site for good/services (i.e., car hire). Authentication at the time of the reservation will allow for future MIT transactions using the reservation pre-authority/mandate when the Customer is not present.	Single	Maximum amount	CIT	Y	0		1 or A	S	0	1, 6, A or S

7.3 Use Cases and POS Data Code Guidance - Online Payments (continued)

Note: 'A' in POS DC1 & 7 denotes Credential on File (COF)

MIT/CIT SCENARIOS												
Case #	**Type**	**Description**	**Transaction**	**Authentication Amount Only**	**MIT/ CIT**	**DF 61 SafeKey**	**DF 113 Initiating Party/Corp. Exemption**	**DF 60 OTID**	**POS DC1**	**POS DC5**	**POS DC6**	**POS DC7**
23	No Show Fees	A Customer does not arrive at a hotel where an authenticated pre-authority/ mandate is in place to allow a fee to be applied.	Single		MIT		1	Y	A	1	0	A
24	Incidental Charges	A Customer incurs incidental charges where an authenticated pre-authority/ mandate is in place to allow a charge to be applied.	Single		MIT		1	Y	A	1	0	A
25	Incremental Charges	A Customer incurs incremental charges where an authenticated pre-authority/ mandate is in place to allow a charge to be applied.	Single		MIT		1	Y	A	1	0	A
26	Multi Sellers	Purchase of multiple supplier goods/services from a single Agent (i.e., Online Retail).	Single	Maximum amount for all goods/ services	CIT	Y	0		1 or A	S	0	1, 6, A or S

7.3 Use Cases and POS Data Code Guidance - Online Payments (continued)

Note: 'A' in POS DC1 & 7 denotes Credential on File (COF)

MIT/CIT SCENARIOS												
Case #	**Type**	**Description**	**Transaction**	**Authentication Amount Only**	**MIT/ CIT**	**DF 61 SafeKey**	**DF 113 Initiating Party/Corp. Exemption**	**DF 60 OTID**	**POS DC1**	**POS DC5**	**POS DC6**	**POS DC7**
27	Split Shipments	Purchase of multiple supplier goods/services from a single Agent (i.e., Online Retail with split shipments).	Single	Maximum amount - Use cryptogram with each authorisation. Total authorisations cannot exceed authentication amount.	CIT	Y	0		1 or A	S	0	1, 6, A or S
28	Third Party Authentication	Authentication of multiple supplier goods/services from a single Agent (i.e., Online Travel Agent).	Single	Maximum amount for all goods/services	CIT	Pass the authentication cryptogram to the authorising Merchant.						
29	Transit Automated Debt Recovery	Card Not Present authorisation request automatically generated in a transit Merchant back office following a declined Card Present transit delayed authorisation request.	Single		MIT		1	Y	A	1		A

7.4 In Case of Outage

If SafeKey or American Express has an outage or technical issue, American Express will take suitable measures to ensure that both the Merchant and the Cardmember are not impacted. In certain outage scenarios, the Merchant may receive an Attempted Authentication Response (ECI 06), and this will require that the Merchant includes SafeKey data (ECI, AEVV, XID) in the Authorisation message.

If the Merchant/their 3DS Provider or Payment Processor has an outage or technical issue, it is the Merchant/processor's responsibility to remediate and ensure that the transaction is sent through with the correct PSD2 SCA requirements.

8.0 PSD2 Data Fields in the Global Credit Authorization Guide

The following data fields must be used with the *Global Credit Authorization Guide* (ISO and XML formats), and outlines the technical requirements to support PSD2.

Data Field 60 NATIONAL USE DATA

Position	Subfield Name	Subfield Length	Subfield Type	Required (M/O/C)	Description
1-3	VARIABLE LENGTH INDICATOR (VLI)	3 bytes	Numeric (EBCDIC)	M	VLI indicates total length of variable data in this data field (not including VLI).
4-5	PRIMARY ID	2 bytes	Alphanumeric	M	Primary ID (Card Type Code) is constant literal "AX" (American Express).
6-8	SECONDARY ID	3 bytes	Alphanumeric	M	Secondary ID (Data Type Code) is constant literal "AAD" (Additional Authorization Data)
9-12	BITMAP IDENTIFIER	4 bytes	Binary (hexadecimal configuration)	M	Bitmap Identifier Each bit in this data element identifies the presence (value 1) or absence (value 0) of a subfield. Following the Bitmap, the layout consists of at least (1) of the following subfields. Each bit position of the 32 bit/4-byte bitmap represents which market specific data are present. If a bit is "ON" in the bitmap, that corresponding subfield will be present.
Subfield					
1	Reserved for American Express Internal Use	N/A	N/A	N/A	N/A
2	Seller ID	20 bytes fixed	Alphanumeric	C[1]	20-digit, Seller ID, that uniquely identifies a Payment Aggregators or OptBlue Participant's specific Seller or Vendor. Left justified, character space filled. This should be the same unique value used to identify a particular Seller when requested in any other American Express message.
LLVAR	Variable Length Indicator	2 bytes	Numeric	C[2]	VLI indicates total length of Seller Email Address variable data.
3	Seller Email Address	40 bytes max	Alphanumeric & special characters	C[1]	Email of the Payment Aggregators or OptBlue Participant's Seller.
4	Seller Telephone	20 bytes fixed	Alphanumeric	C[1]	Telephone number of the Payment Aggregators or OptBlue Participant's Seller. Left justified, character space filled.

C[1] = Mandatory for Payment Aggregators and OptBlue Participants

C[2] = Mandatory if populating Subfield 3, Seller Email Address

8.0 PSD2 Data Fields in the Global Credit Authorization Guide (continued)

Data Field 60 NATIONAL USE DATA (continued)

Position	Subfield Name	Subfield Length	Subfield Type	Required (M/O/C)	Description
Subfield					
5	TOKEN REQUESTOR ID (TRID)	11 bytes, fixed	Alphanumeric	C[3]	Token Requestor ID (TRID) contains the 11-byte numeric value that uniquely identifies the Payment Token requestor. Refer to the *EMVCo Payment Tokenization Specification - Technical Framework* specification for additional information.
6	LAST 4 PAN RETURN INDICATOR	1 byte	Alphanumeric	O	Last 4 PAN Return Indicator is constant literal "**Y**".
7	**Original Transaction Identifier (OTID)**	**15 bytes, fixed**	**Alphanumeric**	**C[4]**	**Original Transaction Identifier associated to the Customer-Initiated Transaction setting up the MIT mandate.**

C[3] = Mandatory for Payment Token transactions where the Token Requestor ID (TRID) is requested.

C[4] = Mandatory for Merchant-Initiated Transactions.

Note: The OTID will be returned with no alteration if populated in Data Field 60 of the Authorization Request message.

8.0 PSD2 Data Fields in the Global Credit Authorization Guide (continued)

DATA FIELD 113	ACCEPTANCE ENVIRONMENT DATA
Length of Field:	17 bytes, LLLVAR
Field Type:	Alphanumeric

Acceptance Environment Data

Position	Subfield Name	Subfield Length	Subfield Type	Required (M/O/C)	Description
1-3	VARIABLE LENGTH INDICATOR (VLI)	3 bytes	Numeric (EBCDIC)	M	VLI indicates total length of variable data in this data field (not including VLI).
4-5	PRIMARY ID	2 bytes	Alphanumeric	M	Primary ID (Card Type Code) is constant literal "AX" (American Express).
6-8	SECONDARY ID	3 bytes	Alphanumeric	M	Secondary ID (Data Type Code) is constant literal "AED" (Acceptance Environment Data)
9	INITIATING PARTY INDICATOR	1 byte	Alphanumeric	M	Indicator that communicates if the Authorization was initiated by the Cardholder (Cardmember-Initiated Transaction (CIT) or the Merchant-initiated Transaction (MIT). Valid values include: 0 = Customer-Initiated 1 = Merchant-Initiated
10-13	BITMAP IDENTIFIER	4 bytes	Binary (hexadecimal configuration)	M	Bitmap Identifier Each bit in this data element identifies the presence (value 1) or absence (value 0) of a subfield. Each bit position of the 32 bit/4-byte bitmap represents which market specific data are present. If a bit is "ON" in the bitmap, that corresponding subfield will be present.

See Subfield table on the next page.

8.0 PSD2 Data Fields in the Global Credit Authorization Guide (continued)

DATA FIELD 113 ACCEPTANCE ENVIRONMENT DATA (continued)

Acceptance Environment Data (continued)

Position	Subfield Name	Subfield Length	Subfield Type	Required (M/O/C)	Description
Subfield					
1	Reserved for future use	1 byte	Alphanumeric	N/A	Reserved for future use.
2	Secure Corporate Payment process and protocol exemption	1 byte	Alphanumeric	C	EU PSD2 Strong Consumer Authentication (SCA) indicator that indicates if the Authorization is not subject to the SCA PSD2 requirements due to the Secure Corporate Payment process and protocol exemption. Valid values include: 0 = Not claimed 1 = Claimed
3	Reserved for future use	1 byte	Alphanumeric	N/A	Reserved for future use.
4	Reserved for future use	1 byte	Alphanumeric	N/A	Reserved for future use.

Note: This field will be returned in the Authorisation Response if provided in the Authorisation Request message.

9.0 American Express SafeKey Comparison Chart

The following table shows the features for SafeKey 1.0 and SafeKey 2.0.

Features	SafeKey 1.0	SafeKey 2.0	
		SafeKey 2.1 EMV 2.1.0	SafeKey 2.2 EMV 2.2.0
Based on industry-standard EMV 3-D Secure	X	X	X
Extra layer of security at check out	X	X	X
Payment authentication	X	X	X
Browser-based authentication	X	X	X
Flexibility for Issuers to use a variety of authentication methods (i.e., one-time passcodes, risk-based decisioning, etc.).	X	X	X
Support for PSD2 compliance	X	X	X
Support for more data elements promoting frictionless authentication	Available in the U.S. and its territories	X	X
App-based (In-App) enablement	—	X	X
Non-payment authentication	—	X	X
Token-based transactions	—	X	X
Out-of-band authentication	—	X	X
Merchant-initiated authentications	—	X	X
Decoupled authentication	—	—	X
PSD2 additional indicators	—	—	X
Request challenge (MIT mandate set-up / PSD2 SCA)	—	X	X
Merchant-Initiated authentications- 3DS Requestor Initiated (3RI) payments and Decoupled	—	—	X

Note: Some of these features may require additional certification.

American Express SafeKey Comparison Chart

this page intentionally left blank

10.0 Indirect Travel Booking Sales

Travel Suppliers (Merchant of Record) must ensure any booking agents who accept bookings or reservations on their behalf complete Strong Customer Authentication and pass all required data fields in scope for SCA.

Travel Management Companies accepting bookings on behalf of corporate clients in a secure and dedicated environment that may benefit from the Corporate Exemption must ensure required exemption data is passed.

The following guidance is for travel & hospitality Merchants and their solution providers to ensure PSD2 compliance is met and to avoid declined payments from transactions via a booking agent (third party agent/indirect sales channel).

The following table lists some of the Merchant Category Codes (MCC) within scope of Travel & Hospitality for indirect sales.

Category	Merchant Category Code (MCC)
Airlines and Air Carriers	4511 and 3000 - 3350
Lodging	7011 and 3501 - 3999
Car Rentals	7512 and 3351 - 3500
Travel Agencies and Tour Operators	4722
Cruise Lines	4411
Transportation Services	4789
Railroads	4011
Ferries	4111
Taxi Cabs and Limousines	4121
Vacation Rental	6513
Motor Home and Vehicle Rent	7519
Trailer Parks and Camp	7033
Bus Lines	4131
Railways	4112

It is important that the Merchant of Record for a card transaction communicates SCA data requirements through their solution providers for indirect sales. If the necessary changes as outlined on the next page are not carried out there is a risk of the transaction being declined by the Card Issuer due to non-compliance.

10.1 Booking Agents

The booking agent is the first point of interaction with the cardholder at time of booking / reservation and is required to be compliant as per the requirements covered in Section 2.0 Strong Customer Authentication Requirements.

Booking agents include any players involved in the booking process if they contribute to the capture and communication of the card details to the travel supplier such as:

- Online Travel Agents (OTA)
- Travel Agents with a web presence
- Travel Management Companies (TMC)
- Central Reservation Systems (e.g. GDS, hotel and car rental)

To meet PSD2 SCA requirements at time of booking, please speak to an approved 3DS solution provider and integrate SafeKey v2+ into your booking tool/ process. Alternatively please ensure you speak to your travel booking tool solution providers to ensure compliance for travel bookings you facilitate.

1. As the booking agent, if you have your own American Express Merchant ID, you can use it to authenticate bookings on behalf of a travel supplier. You will need to ensure the supplier name is provided at time of authentication. Data requirements for this solution are as follows:

3DS Data Field Name	Data Field Requirements
3DS Requestor Name Field Name: threeDSRequestorName	Booking Tool / Travel Agent Name
Merchant Name Field Name: merchantname	Travel Agent Name*Travel Supplier Name or Travel Agent Name*Package Holiday

10.1 Booking Agents (continued)

2. If you do not have an American Express Merchant ID to facilitate an authentication request, then you need to use the American Express 3DS OTA Requestor functionality. Speak to your 3DS Merchant Plug-In (MPI) solution provider who will be able to assist you. Data requirements for this solution are as follows:

3DS Data Field Name	Data Field Requirements
3DS Requestor ID Field Name: threeDSRequestorID	OTA followed by IATA* Agent Number or a unique consistent reference to identify the requestor for the authentication.
3DS Requestor Name Field Name: threeDSRequestorName	Booking Tool/Travel Agent Name
Acquirer Merchant ID Field Name: acquirerMerchantID	Leave blank or use '9999999999'
Merchant Name Field Name: merchantname	Travel Agent Name*Travel Supplier Name or Travel Agent Name*Package Holiday
Acquirer BIN Field Name: acquirerBIN	MPI would need to populate '100000000232'
Merchant Category Code Field Name: mcc	4722 - Travel Agencies and Tour Operators
Merchant Country Code Field Name: merchantCountryCode	Please specify Travel Agent Country Location as per the American Express *Global Codes & Information Guide***.

*International Air Transport Association

** *Global Codes & Information Guide* can be found at www.americanexpress.com/merchantspecs.

10.2 Booking Tool Solution Providers and Travel Intermediaries

The travel booking process has many solution providers and intermediaries that receive and pass travel and payment data from the booking agent to the travel supplier (Merchant of Record) and play a vital role in the booking distribution network.

Solution providers involved in passing travel & hospitality booking and payment details include, but are not limited to:

- Global Distribution Systems (GDS)
- IATA BSP (International Air Transport Association - Billing and Settlement Plan)
- Travel Content Aggregators
- Online Corporate Booking Tools
- Customer Reservation Systems (CRS)
- Property Management Systems (PMS)
- Channel Managers
- Software, Platform and Payment Providers to any of the above solution providers

It is important for solution providers and travel intermediaries to speak with both their clients, the booking agent and all downstream parties through to the travel supplier to ensure all parties can pass the required data fields.

If you provide a card payment authorisation service, then please also speak with your payment gateway or card payment solution provider as the data required to be passed is different.

See table on the next page.

10.2 Booking Tool Solution Providers and Travel Intermediaries (continued)

Booking Scenarios						
Authentication and Authorisation Requirements					Data Required to be Passed through Travel Intermediaries	
Case #	**Type**	**Description**	**Transaction**	**Authentication Amount Only**	**Transaction Type**	**Authentication / Exemption Data to Be Passed**
1	Booking / Reservation via Third Party Agent Online	CM enters Terms and Conditions of Third Party Agent and Agent is not Merchant of Record	Authentication Only and pass 3DS data to Merchant of Record	Full Amount	Internet	3DS Authentication Data: 1. Electronic Commerce Indicator value 2. American Express Verification Value (AEVV) 3. American Express SafeKey Transaction ID (3DS V1 = XID, 3DS V2 = DS Transaction ID)
		Third Party Agent facilitates CIT Authorisation	Initial CIT Nominal amount or zero		Internet	3DS Authentication Data: 1. Electronic Commerce Indicator value 2. American Express Verification Value (AEVV) 3. American Express SafeKey Transaction ID (3DS V1 = XID, 3DS V2 = DS Transaction ID) Authorisation Transaction ID
		Merchant of Record facilitates CIT Authorisation	Initial CIT As per booking Terms and Conditions		Internet	
		Agent is TMC and meets criteria of Corporate Exemption	Corporate Exempt		Internet	Secure Corporate Payment Indicator
2	Booking / Reservation via Third Party Agent Call Centre	Third Party Agent facilitates CIT Authorisation	Initial CIT Nominal amount or zero		Call Centre	MOTO Indicator
		Merchant of Record facilitates CIT Authorisation	Initial CIT As per booking Terms and Conditions		Call Centre	MOTO Indicator
3	Booking / Reservation via Third Party Agent Hight St Face to Face	CM enters Terms and Conditions of Third Party Agent and Agent is not Merchant of Record	Authentication Chip PIN required	Nominal amount or zero	CM Present	Original Transaction ID

10.3 Travel Supplier - Merchant of Record

Travel Suppliers (Merchant of Record) must ensure any booking agents who accept bookings or reservations on their behalf complete Strong Customer Authentication and pass all required data fields in scope for SCA.

Travel Management Companies accepting bookings on behalf of corporate clients in a secure and dedicated environment that may benefit from the Corporate Exemption from SCA must ensure required exemption data is passed.

If authentication has not been actioned by your Booking Agent, your authorisation request is at risk of decline. If you receive a soft decline (Action Code 130) to proceed with the booking you will need to complete authentication utilising a Pay by Link solution or wait until the customer is present to complete a Chip and Pin transaction.

It is recommended that the guidance provided by American Express should be shared with your booking agents to ensure they understand the requirements of SCA.

See the tables on pages 39 - 41.

10.3 Travel Supplier - Merchant of Record (continued)

Booking Scenarios													
Authentication and Authorisation Requirements					Merchant Data Requirements to American Express Issuer								
Case #	**Type**	**Description**	**Transaction**	**Authentication Amount Only**	**MIT/ CIT**	**DF 61 SK**	**DF 113 CIT/MIT/ SCT**	**DF 60 OTID**	**DF 55**	**POS DC1**	**POS DC5**	**POS DC6**	**POS DC7**
1	Booking / Reservation via Third Party Agent Online	CM enters Terms and Conditions of Third Party Agent and Agent is not Merchant of Record	Authentication Only and pass 3DS data to Merchant of Record	Full amount	CIT								
		Third Party Agent facilitates CIT Authorisation	Initial zero or nominal amount		CIT	Y	0			1	S	0	1,6, S or A
		Merchant of Record facilitates CIT Authorisation	Initial CIT As per booking Terms and Conditions		CIT	Y	0			1	S	0	1,6, S or A
		Merchant of Record facilitates MIT Authorisation for subsequent charges	MIT		MIT		1	Y		A	1	0	1,6, S or A
		Agent is TMC and meets criteria of Corporate Exemption	Corporate Exempt				1 See Secure Corporate Exemption (SCT) - Lodged Cards			1	S	0	1,6 or S

10.3 Travel Supplier - Merchant of Record (continued)

Booking Scenarios													
Authentication and Authorisation Requirements					Merchant Data Requirements to American Express Issuer								
Case #	**Type**	**Description**	**Transaction**	**Authentication Amount Only**	**MIT/ CIT**	**DF 61- SK**	**DF 113- CIT/MIT/ SCT**	**DF 60 OTID**	**DF 55**	**POS DC1**	**POS DC5**	**POS DC6**	**POS DC7**
2	Booking/ Reservation via Third Party Agent Call Centre	CM enters Terms and Conditions of Third Party Agent and Agent is not Merchant of Record	No authentication required										
		Third Party Agent facilitates CIT Authorisation	Initial zero or nominal amount		CIT		0			1	3	0	1,6,S or A
		Merchant of Record facilitates CIT Authorisation	Initial CIT As per booking Terms and Conditions		CIT		0			1	3	0	1,6,S or A
		Merchant of Record facilitates MIT Authorisation for subsequent charges	MIT		MIT		1	Y		A	1	0	1,6,S or A

10.3 Travel Supplier - Merchant of Record (continued)

Booking Scenarios													
Authentication and Authorisation Requirements					Merchant Data Requirements to American Express Issuer								
Case #	**Type**	**Description**	**Transaction**	**Authentication Amount Only**	**MIT/ CIT**	**DF 61-SK**	**DF 113-CIT/MIT/ SCT**	**DF 60 OTID**	**DF 55**	**POS DC1**	**POS DC5**	**POS DC6**	**POS DC7**
3	Booking / Reservation via Third Party Agent High St Face to Face	CM enters Terms and Conditions of Third Party Agent and Agent is not Merchant of Record	Card Present Chip and PIN/ Digital Wallet Section 7.2 High Level Transaction Types and POS Data Code Values	Zero or nominal amount	CIT		0		Y	5	0	1 or Z	1,6,5 or A
		Merchant of Record is responsible to facilitate CIT Authorisation using authentication with Pay by Link	Initial CIT As per booking Terms and Conditions		CIT	Y	0			1	S	0	1,6,S or A
		Merchant of Record facilitates MIT Authorisation for subsequent charges	MIT		MIT		1	Y		A	1	0	1,6,S or A

Important Note: Please contact your American Express representative if a third party booking agent, solution provider or intermediary is not able to send authentication data through to the travel supplier (Merchant of Record). It is possible to pass as MIT, or MOTO when MIT is not possible in the interim. See Section 6.0 Out of Scope Transactions (Merchant-Initiated Transactions) or Section 4.4 Mail Order and Telephone Order (MOTO Transactions) of the main guide.

10.4 Direct Sales Travel Use Cases

Below are some use cases to highlight how SCA can be carried out and the data to be provided when the Merchant is managing the booking and the payments entirely.

Booking Scenarios													
Case #	**Type**	**Description**	**Transaction**	**Authentication Amount Only**	**MIT/ CIT**	**DF 61- SK**	**DF 113- CIT/MIT/ SCT**	**DF 60 OTID**	**DF 55**	**POS DC1**	**POS DC5**	**POS DC6**	**POS DC7**
1	Full Payment Internet	Cardholder purchasing direct on Travel Supplier Website. Refer to Section 4.0 New Regulatory Landscape for Remote Transactions and Actions.	Single	Full Amount		Y				1	S	0	1,6,S
2	Reservation - Advance Deposit Customer goes online to book for themselves. Only a Deposit is taken at the beginning and the remaining payment by the Travel supplier at a later stage.	Refer to Section 6.0 Out of Scope Transactions (Merchant-Initiated Transactions).	Initial	Maximum Amount (authentication for £1000 but £100 taken for payment) Needs to be clearly stated in Terms and Conditions	CIT	Y	0			1	S	0	1,6,S or A
			Subsequent	Different amounts depending on payment terms	MIT		1	Y		A	9	0	A
			Subsequent	Final payment	MIT		1	Y		A	1	0	1,6,S or A

10.4 Direct Sales Travel Use Cases (continued)

Booking Scenarios													
Case #	**Type**	**Description**	**Transaction**	**Authentication Amount Only**	**MIT/ CIT**	**DF 61- SK**	**DF 113- CIT/MIT/ SCT**	**DF 60 OTID**	**DF 55**	**POS DC1**	**POS DC5**	**POS DC6**	**POS DC7**
5	Customer walks into Travel Supplier Bricks and Mortar	Card Present Chip and Pin / Contactless / Digital Wallet. Refer to Section 7.2 High Level Transaction Types and POS Data Code Values.	Single	Full amount	CIT		N/A		Y	5	0	1,X or Z	5
6	Customer Checks in online / Loyalty storing of card	SCA for the initial storing of the card	Initial	Zero or nominal amount	CIT	Y	0			1 or A	S	0	1,6,S or A
			New online booking	Full amount	CIT	Y	0			1 or A	S	0	1,6,S or A
			Initial	Varied	MIT		1	Y		A	1 or 9	0	A
7	Customer checks in F2F	Incidental charges	Subsequent	Varied	CIT				Y	5	0	1,X or Z	5

this page intentionally left blank

11.0 Countries Subject to SCA

The following table shows the countries where American Express expects Merchants to allow SCA to be performed by the Issuer.

Countries
Aland Islands
Andorra
Austria
Azores
Belgium
British Antarctic Territory
British Indian Ocean Territory
Bulgaria
Canary Islands
Croatia
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
French Guiana
Germany
Gibraltar
Greece
Guadeloupe
Holy See (Vatican City State)
Hungary
Iceland
Italy

Countries
Latvia
Lichtenstein
Lithuania
Luxembourg
Madeira
Malta
Martinique
Mayotte
Monaco
Netherlands
Norway
Pitcairn Islands
Poland
Portugal
Republic of Ireland
Reunion
Romania
San Marino
Slovakia
Slovenia
Saint Martin
Spain
Sweden
United Kingdom
Wallis and Futuna

this page intentionally left blank

12.0 Revision Log

The Revision Log goes back three publications, current publication plus the last two. For earlier versions, contact SpecQuestions@aexp.com.

The Revision Log contains a condensed overview of the *PSD2 Guide - Including Travel* changes. The Revision Log is divided into the following types of changes:

- General - Changes made due to reorganization, clarification, consistency, or for informative purposes
- Global - Changes made in multiple locations, not specific to a data field
- Specific data field changes - Changes made to specific data field(s) as noted
- Specific section changes - Changes made to specific section(s) as noted

Publication: October 2020 | Global Data Quality & Standards (GDQ&S) | Contact: SpecQuestions@aexp.com

Type of Change/ Message Type	Data Field (DF)/ Section # / Title	Description
Specific Section Changes	Cover Page and Header	Changed the Cover page and header information to 'PSD2 Guide - Including Travel' (no revision marks for this entry).
	Section 1.3 Document Changes	Updated to align with new document title.
	Section 3.5 Unattended Terminals for Transport Fares and Parking Fees	For MCC Codes 7523 and 4784, in the POSDC4 column, added 'Z'.
	Section 4.2 SCA Requirements in a Remote Environment	For SCA Required, changed bullet to 'Electronic commerce (POS DC 4 or 5, value "S") bearing the SafeKey cryptogram provided during the authentication process'.
	Section 5.4 Corporate Exemption	In the first paragraph, changed the last sentence to 'These are often referred to as "lodged cards" and typically are Business to Business relationships. Examples include but are not limited to: Travel Management Companies and Corporate Buyer / Supplier Relationships'.
		Reworded the last paragraph.
	Section 5.5 Credential on File	Updated section.
	Section 6.2 Transaction ID and Original Transaction ID	In the first paragraph, changed the last sentence to 'For additional information, refer to the Global Credit Authorization Guide., ISO and XML formats'.
	Section 6.3.5 Reauthorisation	Changed the second sentence to 'Common instances that require reauthorisations include delayed shipments, split shipments, extended stays, extended rentals and debt recovery'.

12.0 Revision Log (continued)

Publication: October 2020 (continued)

Type of Change/ Message Type	Data Field (DF)/ Section # / Title	Description
Specific Section Changes (continued)	Section 6.4 MIT Transactions and Authorisation Specification Changes	Reworded the second paragraph.
	Section 7.0 High Level Transaction Types and POS Data Code Values	In the first table, changed 'Digital Wallet' to 'Digital Wallet - In App'.
		Moved Digital Wallet to the third table.
	Section 7.2 High Level Transaction Types and POS Data Code Values	In the first table, changed 'Digital Wallet' to 'Digital Wallet - In App'.
		Moved Digital Wallet to the third table.
		In the Merchant-Initiated Transaction - Credential on File table, added the following and highlighted the applicable values 'Note: If not supporting DF113, American Express will on an interim basis accept the fields highlighted as MIT. Please note that if no OTID is present the CIT and MIT must have the same MID for authorisation'.
	Section 7.3 Use Cases and POS Data Code Guidance - Online Payments	Changed the description for Dynamic Linking to 'Transactions for which the final amount is unknown: UK Finance have published guidance for **UK issued cards** only confirming that a tolerance between authentication and authorisation is acceptable if within the payer's reasonable expectations. The % tolerance will be aligned with the current American Express Estimated Charge Policy. Please note: This approach still requires FCA approval. **EEA issued cards** (excluding UK) cannot benefit from any tolerance'.
		For Case #28 Third Party Authentication, merged DF61, DF113, DF60 and DF22 positions.
		Added Case #29 Transit Automated Debt Recovery.
	Section 9.0 American Express SafeKey Comparison Chart	In the American Express SafeKey Comparison Chart, added rows for 'Request challenge (MIT mandate set-up / PSD2 SCA)' and 'Merchant-Initiated authentications - 3DS Requestor Initiated (3RI) payments and Decoupled'.
	Section 10.0 Indirect Travel Booking Sales	Added section.
	Section 11.0 Countries Subject to SCA	Added section.

12.0 Revision Log (continued)

Publication: February 2020 | Global Data Quality & Standards (GDQ&S) | Contact: SpecQuestions@aexp.com

Type of Change/ Message Type	Data Field (DF)/ Section # / Title	Description
Global Changes	Multiple Locations	Changed references of 'Card on File' to 'Credential on File'.
Specific Section Changes	Summary of Changes Table	Added Summary of Changes Table.
	Section 1.0 About the Revised Payment Services Directive	Changed the second sentence to 'The regulator has agreed to a managed roll out of the SCA requirements for electronic commerce transactions'.
	Section 1.3 Document Changes	Added section and renumbered accordingly.
	Section 1.4 Related Documents	Added bullets for the following documents: • *EMV 3-D Secure Protocol and Core Functions Specifications v2.X* • *American Express 2.0 Protocol specification version 2.10* • *American Express SafeKey 2.0 Acquirer-Merchant Implementation Guide*
	Strong Customer Authentication Requirements	In the sixth paragraph, changed '(also known as white listing)' to '(also known as whitelisting or Express List for American Express)'.
	Section 4.2 SCA Requirements in a Remote Environment	Updated the section.
	Section 4.3 Failure to Satisfy SCA Requirements in a Remote Environment	Changed the section heading.
	Section 5.1 Low Value Transactions	Added sentence 'At this stage, American Express does not require a low value exemption indicator in the Authorisation message'.
	Section 5.2 Transaction Risk Analysis	Add the sentence 'At this stage, American Express does not require a transaction risk analysis exemption indicator in the Authorisation message'.

12.0 Revision Log (continued)

Publication: February 2020 (continued)

Type of Change/ Message Type	Data Field (DF)/ Section # / Title	Description
Specific Section Changes	Section 5.3 Trust Beneficiaries	Changed the last sentence to 'At this stage, American Express does not require a trusted beneficiary indicator in the Authorisation message'.
	Section 5.4 Corporate Exemption	Updated the section.
	Section 5.5 Credential on File	Added new section.
	Section 6.1 MIT Mandate / Pre-Authorisation	Added heading and the third paragraph.
	Section 6.2 Transaction ID and Original Transaction ID	Added new section.
	Section 6.4 MIT Transactions and Authorisation Specification Changes	Added new section.
	Section 7.2 High Level Transaction Types and POS Data Code Values	Updated the tables.
	Section 7.3 Use Cases and POS Data Code Guidance - Online Payments	Added a bullet above the table for Dynamic Linking.
		Updated the tables.
	Section 8.0 PSD2 Data Fields in the Global Credit Authorization Guide	Added new section.
	Section 9.0 American Express SafeKey Comparison Chart	Added new section.

12.0 Revision Log (continued)

Publication: July 2019 | Global Data Quality & Standards (GDQ&S) | Contact: SpecQuestions@aexp.com

Type of Change/ Message Type	Data Field (DF)/ Section # / Title	Description
Initital release.		

this page intentionally left blank