Global Payments

Stored Credential Technical Implementation Guide V1.8

October 2021

globalpayments Innovation that delivers.

Amendment History

Version	Status	Date Issued	Comment	Originator	Reviewed By
1.0	New	10/07/2017	Issued By Global Payments	Core Product	Marketing Operations
1.1	Update	19/10/2017	Erroneous 'Note' removed from General Sub Record 01. Additional values removed from Payment Attributes Data Values table.	Core Product	Marketing Operations
1.2	Update	14/03/2018	Update to include Mastercard's requirements. Corrections made to cardholder initiated transaction examples in Appendix C.	Product Compliance	Core Product
1.3	Update	12/04/2019	Updated to include Strong Customer Authentication requirements.	Product Compliance	Marketing
1.4	Update	16/10/2019	Change of address in footer.	Product Compliance	Marketing
1.5	Update	14/02/2020	Updated guidance on Customer Initiated Transactions and a new summary section. (Section 4)	Product Compliance	Marketing
1.6	Update	05/08/2020	Expansion to include American Express. Explicit explanation of MITs. Explanation of need for SCA exemption flags. Addition of SCA Exemption Flags in appendices. Simplification of Appendix C	Product Compliance	Testing & Schemes
1.7	Update	16/04/2021	Updates to ensure consistency with ASTS v2.1. Change in guidance and clarification on SCA Exemption flagging in settlement in Sub-Record 41	Schemes Consultancy	Testing & Schemes
1.8	Update	16/10/2021	Update with new template. Changes to Appendix B to reflect changes to Sub-Record Type 41 in the ASTS and the creation of Table 17 in the ASTS. Additional Appendix D with guidance on correct values for token transactions.	Schemes Consultancy	Testing & Schemes

Contents

1. Introduction

The Card Schemes (Visa, Mastercard and American Express) have defined mandatory rules and processing specifications for transactions performed using stored card details. As card details could either be normal card numbers or tokens, the card details for the purpose of this document will be referred to as credentials.

This document provides the data values (Stored Credential Indicators) required by the card schemes to identify the initial storage and the subsequent usage of stored credentials. It should be read in conjunction with our *Authorisation And Settlement Technical Specifications (ASTS) Guide.* The data values need to be submitted in both the authorisation and settlement messages. Appendix A contains the additional data values required in the authorisation message. Appendix B contains the additional data values required in the settlement message.

The *ASTS Guide* is available by calling our helpdesk on 0345 702 3344* or by speaking to your Relationship Manager.

To avoid confusion and prevent errors, please implement these changes for all card types and our systems will then correctly flow the relevant card data values to the card schemes, as appropriate.

Visa also mandate that cardholder consent is obtained for storage of their credentials. Details of what's needed for the consent agreement can be found in the *Stored Credential Guide.* This is located in the Help Centre section of our website at **www.globalpaymentsinc.co.uk/en-gb**. You'll find it within the Stored Credential Transaction option.

Since **14th September 2019**, the Payment Services Directive 2 (PSD2) has mandated that all Customer Initiated payments have to be validated using Strong Customer Authentication (SCA). Although the enforcement has been delayed in the UK, card issuers are obliged to seek SCA or decline in scope transactions that aren't fully authenticated. It's now more critical than ever that Stored Credential Transactions are flagged correctly (including the SCA Exemption Flags). Merchant Initiated Transactions do not require authentication, but if the issuer cannot identify them correctly, the card issuer may choose to challenge the transaction and request SCA., and if the cardholder can't be contacted or can't provide SCA, the transaction won't go ahead. Version 1.6 of this guide made it explicit the expected SCA Exemption flagging that should be present

For more details on SCA, how it works and what's required, see our *PSD2 and Strong Customer Authentication Technical Implementation Guide*, which is also on our website within our Help Centre. You'll find it under the option for Strong Customer Authentication.

This document is subject to regular change and update due to the changing nature of card scheme rules and specifications, especially with tokenisation of card PANs and the development of Secure Remote Commerce.

2. Transaction Types

This section details the transaction types that are impacted by the card scheme's requirements. Stored credential transactions (also called Credential on File (CoF) transactions) are split into two distinct types:

- Cardholder Initiated Credential on File transactions, and
- Merchant Initiated Credential on File transactions.

2.1 Cardholder Initiated Credential on File Transactions

A Cardholder Initiated Transaction (CIT) is any transaction where the cardholder is actively participating in the transaction. This can be either at a card terminal in a store, over the telephone, through a checkout online or even by post. In the subsequent Credential on File CIT scenario, the cardholder isn't present, but initiates a transaction where they don't need to enter their card details as the merchant uses the card details previously stored by the cardholder to perform the transaction.

All CITs are subject to SCA requirements and should be authenticated with 3D Secure whether it's the initial or subsequent transaction, unless an SCA exemption is requested or the transaction type is out of scope for SCA, for example, Mail Order/Telephone Order (MOTO) transactions.

Transactions that fall within the CIT type are limited to normal Sale, Pre-authorisation and Account Verification transaction types.

With version 1.5 of this document Global Payments no longer mandated the submission of Scheme Reference Data from the initial transaction with subsequent Cardholder Initiated Transactions. (Below)

2.2 Merchant Initiated Credential on File Transactions

A Merchant Initiated Transaction (MIT) is commonly initiated by a merchant without any active participation from the cardholder. To do this, the cardholder would have previously needed to give the merchant consent to store their card details. Following PSD2 regulations and card scheme rules, the customer must also be fully authenticated before a MIT may take place. This means that a MIT can only happen after a CIT of some kind has taken place first. MITs can be split into two kinds of transactions:

- Standing Instructions
- Industry Practices

1. Standing Instructions

Transactions that reuse the cardholder's credentials either on a regular fixed period or, when a certain event occurs. Standing Instructions are defined as the following types of transaction:

- **Recurring Payments** – transactions that are processed on a regular fixed interval for a **fixed** pre agreed amount. Recurring Transactions don't have a fixed duration and will continue to be processed until the cardholder cancels the agreement.
- **Instalment Payments –** transactions that are processed on a regular fixed interval for a pre agreed amount. Unlike Recurring Transactions, Instalments do have a fixed duration and mustn't continue to be processed after the end of the agreed instalment period.
- **Unscheduled Credential on File Transactions –** transactions that are for a fixed or variable amount that don't occur on a scheduled or regularly occurring transaction date, but when a pre-defined event happens. For example, an account automatic top up when it falls below a minimum balance.

2. Industry Practice Transactions

Transactions that reuse the cardholder's credentials on an unscheduled and often one-off occurrence, with prior consent from the cardholder. Industry Practice Transactions are defined as the following types of transaction:

- **Incremental Authorisations** – used to increase the total amount authorised if the original authorisation amount is insufficient.
- **Resubmissions** – used when the original authorisation has been declined for insufficient funds.
- **Reauthorisations** – used when the validity period for a previous authorisation has expired.
- **Delayed Charges** – used to process an additional charge after the original transaction has been completed.
- **No Show** – used to charge a cardholder a penalty for not showing up for a reservation or a late cancellation in accordance with the merchant's cancellation policy.

All the above are exempt from SCA as long as they are flagged correctly as MITs with the appropriate exemption flag (depending on whether the amount was fixed or variable). If incorrect flagging is used, then the card issuer may request SCA to be performed, which won't be possible if the customer isn't actively participating in the transaction and would lead to the transaction being declined.

2.3 In-app transactions.

In-app transactions made using a customer's card details which entered into the app and are then stored for use by either the customer or the merchant to initiate future transactions are to be treated as per ecommerce transactions in this document.

In-app transactions can also be performed using a token wallet (such as Apple Pay) to pay for the first CIT transaction. **Visa does not permit such a token to be stored for to be used for future MITs**. Mastercard however currently does permit this. See Appendix D for how such transactions should be submitted.

2.4 Other tokenised transactions

Merchants together with their PSPs may choose to tokenise the stored card with the appropriate card scheme after authenticating the customer through the first transaction. Specific care should be paid to how token transactions are submitted in authorization. See the ASTS for details. CITs are still subject to SCA even those performed with stored PANS.

3. Message Formats to Be Used for Credential on File Transactions

This section provides details of when to use the appropriate data values. Examples of the data values that are needed on some transaction types can be found in Appendix C.

We require that you, or the company that you have a contract with for providing your equipment/service, complete testing with us before the changes are implemented. Testing can be arranged through your equipment provider/service provider or Relationship Manager.

3.1 Authorisation

3.1.1 Storing a Credential for the First Time

The first transaction in the series of transactions will store the cardholder's credentials securely within the merchant's system.

The first transaction may be one of the following:

- A face to face chip and PIN or
- A face to face contactless transaction (if authentication took place using a device), or
- A MOTO transaction, or
- A fully authenticated ecommerce transaction.

If a payment, or the first payment in a series of payments, is to be taken at the time of the first transaction, the transaction must be completed for the agreed amount.

If a pre-authorisation is to be taken at the time of the first transaction, the authorisation must be completed for the estimated amount.

If a payment or pre-authorisation isn't being undertaken at the time of the first transaction (for example, setting up a series of payments for a magazine subscription that commences in one month's time) the first authorisation must be an Account Verification Transaction with a zero value (see the *ASTS Guide* for full details of Account Verification Transactions). Merchants choosing to do these types of transactions should discuss this with Global Payments, as Visa mandates that the first full priced transactions following an introductory offer or free period should be marked as such on the card holder's statement. There is a specific standalone guide to explain this available on request.

When storing a credential for the first time, it's important that Scheme Reference Data from the initial transaction is retained and resubmitted with any subsequent Merchant Initiated Transaction made using the stored credential (see the *ASTS Guide* for full details of how to receive and submit Scheme Reference Data).

The data values to indicate that a credential is being stored for the first time are sent in the authorisation request message in the Payment Attributes Auxiliary Data Record (see Appendix A – Authorisation Auxiliary Data Records). When the credential is stored for the first time, the following data values must be set in the Payment Attributes Field:

- Position 1 – Set as appropriate for the transaction type
- Position 2 – Set as appropriate for the transaction type
- Position 4 – Set to 'F'

3.1.2 Performing Transactions Using Stored Credentials

As stated above, when performing a transaction using a stored credential, it's important that the Scheme Reference Data from the initial transaction is included for all Merchant Initiated Transactions (see the *ASTS Guide* for full details of how to receive and submit Scheme Reference Data).

The data values to indicate that a stored credential is being used are sent in the authorisation request message in the Payment Attributes Auxiliary Data Record (see Appendix A – Authorisation Auxiliary Data Records). For using the credential for subsequent transactions, the following data values must be set in the Payment Attributes Field:

- Position 1 – Set as appropriate for the transaction type
- Position 2 – Set as appropriate for the transaction type
- Position 4 – Set to 'S'

It is important to note that MITs are not ecommerce transactions and should not be flagged as such in either authorisation or settlement. It is both unfortunate and confusing that the SCA exemptions required were added to the ecommerce message blocks in both authorisation and settlement messages, but they should not be considered as ecommerce. Flagging using ecommerce values (other than those specified in Appendix A) will lead to transactions being rejected by card scheme edits.

MITs should be set as Message Type A0 and not B2 (ASTS Table 2) unless they are account verification messages in which case the appropriate 'E' Message Type should be used

3.2 Settlement

When sending a transaction relating to a stored credential, either when storing the credential for the first time or reusing a previously stored credential, additional data values must be included in the Payment Attributes Field of the General Sub Record, which may or may not already be part of the transaction record for other reasons.

The scheme reference data submitted in the settlement record should be that returned in the associated authorisation response.

The format and data values for the General Sub Record can be found in Appendix B.

Note: Payment Attributes Field data values for authorisation and settlement transactions are subtly different and, therefore, care must be taken to use the correct data values from the correct table.

3.2.1 Storing a Credential for the First Time

The Customer Instruction Value in Segment 1 will reflect how the initial transaction was performed, e.g. 'G' for fully authenticated ecommerce.

3.2.2 Performing Transactions Using Stored Credentials

If the transaction was a CIT ecommerce transaction then it will either be subject to SCA or have been exempted from SCA exemption, The Customer Instruction Value in Segment 1 will reflect how the CIT transaction was performed, e.g. 'G' for fully authenticated ecommerce

It is important to note that MITs are not ecommerce transactions and should not be flagged as such in the settlement message. It is unfortunate and confusing that the SCA exemptions required were added to the ecommerce message blocks in both authorisation and settlement but they should not be considered as ecommerce. Using ecommerce values (other than those specified in Appendix B) will lead to transactions being rejected by card scheme edits.

The Customer Instruction Value in Segment 1 must be '2' Continuous Authority for all MITs.

If the Customer Instruction Value is 2 – Continuous Authority, then the second position of the Payment Attributes (Table 12 of the ASTS) is 'C' cardholder not present (unspecified). It should never be 'E' or 'N' when the Customer Instruction value is 2

Summary of Key Principles For Stored Credential Transactions After PSD2 is implemented

4.1 Key Principles

- The first transaction in a series of stored credential transactions:
    - Is the time when the customer enters into an agreement with the merchant and agrees to have their data stored.
        - Is subject to SCA (unless it is a MOTO transaction -which is currently out of scope for SCA)
    - Is flagged with an 'F' in position 4 of the Payments Attributes.
- A merchant must store the Scheme Reference Data returned in the authorisation response from the first transaction. (See below).
- If the stored credential transaction is MOTO, it must:
    - Be flagged as mail order or telephone order in position 2 of the Payments Attributes.
    - Be flagged as Message Type '09' in the authorisation request. (See Table 2 of the ASTS.)
- All subsequent transactions in a series of stored credential transactions must:
    - Be flagged with an 'S' in position 4 of the Payments Attributes
- Subsequent transactions in a stored credential transaction series that are Customer Initiated Transactions must be subject to SCA (unless an explicit waiver is requested – for example a 'low value transaction' waiver. They should be formatted as any other 3DS ecommerce transaction (using, for example Auxiliary Data Record 0101) with the addition of the Payment Attribute flags. GPUK no longer mandates the submission of the Scheme Reference Data from the original transaction for Customer Initiated Transactions.
- Subsequent transactions in a stored credential transaction series that are Merchant Initiated Transactions are SCA exempt and must:
    - Be flagged with an SCA exemption flag in the authorisation request (Auxiliary Data Record 0101) and (in some circumstances) settlement (Sub Record Format Type 41)
    - Have the correct Payment Attribute flags in both the authorisation and settlement messages.
    - Have the Scheme Reference Data returned from the first authorisation submitted in the authorisation request and the Scheme Reference Data returned in the authorisation response submitted in the settlement message. (See below).
- Merchant Initiated Transactions are not ecommerce transactions although they do require the use of ecommerce data blocks to carry SCA Exemption flags.

4.2 Scheme Reference Data

Scheme Reference Data is needed by an issuer for 2 things:

- in an authorisation request it links back to a previously approved authorisation request:
    - for incremental authorisations to tie them together
    - in CoF - to tie subsequent SCA exempt transaction back to the original when SCA was applied (unless MOTO)
- in settlement it allows the card scheme and the issuer to match the settlement amount with the reserved funds from the authorisation.

The Scheme Reference Data to be submitted in an authorisation request is a minimum 15 characters long.

- The Mastercard Trace ID is 15 characters long.
- The Visa Scheme Reference Data returned in an authorisation response is 19 characters long comprised of the 15 character Transaction ID and the 4 character long Validation ID. Merchants are not required to send back the Validation ID, although the authorisation request will not be rejected if they do so
- The American Express Original Transaction Identifier is 15 characters long.

Appendix A – Authorisation Auxiliary Data Records

All stored credential authorisations require specific flags in Auxiliary Data Record Type 18.
Subsequent MIT transactions require SCA exemption flags setting in Auxiliary Data Record 0101

Stored Credential Flags

Type 18: Payment Attributes

Num	Name	F/V	Type	Len	M/O/C	Comment
31.3	Auxiliary Data Record					
31.3.1	Record Separator	F	RS	1	M	1E (HEX)
31.3.2	Auxiliary Data Record Type	F	A	2	M	'18'
31.3.3	Auxiliary Data Record Sub-Type	F	N	2	M	'01'
31.3.4	Group Separator	F	GS	1	M	1D (HEX)
31.3.5	Payment Attributes	F	AB	24	M	See table below

Payment Attributes Data Values (to Be Used in Field 31.3.5)

Table 13 of the ASTS (below) specifies the possible values to be set in the Payment Attributes.
Positions 3 and 5 are not normally required for standard stored credential transactions and should be defaulted to N or space filled.

Posn.	Attribute	Value	Meaning
1	Card Acceptor/Cardholder Agreement (see Note 1)	A	Re Authorisation
		C	Unscheduled Payment
		D	Delayed Charges
		I	Instalment
		L	Incremental
		N	Not Applicable
		R	Recurring Payment
		S	Re Submission
		X	No show
2	Cardholder Not Present Condition (see Note 2)	C	Cardholder Not Present (unspecified)
		M	Mail Order
		N	Not Applicable (i.e. cardholder present)
		T	Telephone Order

Posn.	Attribute	Value	Meaning
		E	Electronic Commerce
3	Debt Repayment (see Note 3)	D	Debt Repayment
		N	Not Applicable
4	Stored Payment Details Indicator	F	Payment Details Stored for First Time
		N	Not Applicable
		S	Using Previously Stored Payment Details
5	Additional Authorisation Condition Indicator (See Note 3)	D	Deferred Authorisation
		N	Not Applicable
6	Reserved For UK Finance		
7	Reserved For UK Finance		
8	Reserved For UK Finance		
9	Reserved For UK Finance		
10	Reserved For UK Finance		
11	Reserved For UK Finance		
12	Reserved For UK Finance		
13	Reserved For UK Finance		
14	Reserved For UK Finance		
15	Reserved For UK Finance		
16	Reserved For UK Finance		
17	Reserved For UK Finance		
18	Reserved For UK Finance		
19	Reserved For UK Finance		
20	Reserved For UK Finance		
21	Reserved For UK Finance		
22	Reserved For UK Finance		
23	Reserved For UK Finance		
24	Reserved For UK Finance		

Note 1: Values other than N only to be used with cardholder present, cardholder not present, continuous authority or electronic commerce sale message types.

Note 2: Values other than N only to be used with cardholder not present or electronic commerce message types

Note 3: The default value of this field is ‘N’. The value ‘D’ is restricted to specific merchant categories and should only be used after consultation with Global Payments. If the field is not populated with an ‘N’ or ‘D’ it must be space filled.

SCA Exemption Flags

Type 01: Ecommerce

Stored Credential Transactions may or may not be ecommerce transactions:

Initial Customer Initiated Transactions must be subject to SCA (unless out of scope). Subsequent Customer Initiated Transactions mostly will be ecommerce and are subject to SCA (unless an exemption is requested). All the values in Auxiliary Record 0101 should be populated as per the ASTS.

Merchant Initiated Transactions are not e-commerce transactions but require some fields of the Auxiliary Data Record 0101 to be set. The format for record 0101 to be used for subsequent MIT authorisation requests sent straight to authorisation is specified in the table below.

When a MIT exemption is requested from an Issuer ACS then Auxiliary Record 0101 should be populated fully as per the ASTS.

Num	Name	F/V	Type	Len	M/O/C	Value needed for MIT transactions
31.3	Auxiliary Data Record					
31.3.1	Record Separator	F	RS	1	M	1E (HEX)
31.3.2	Auxiliary Data Record Type	F	A	2	M	'01'
31.3.3	Auxiliary Data Record Sub-Type	F	N	2	M	'01'
31.3.4	Group Separator	F	GS	1	M	1D (HEX)
31.3.5	Additional Transaction Security Data	F	H	6	M	D08000
31.3.6	Group Separator	F	GS	1	C_1	1D (HEX)
31.3.8	Group Separator	F	GS	1	C_1	1D (HEX)
31.3.10	Group Separator	F	GS	1	C_1	1D (HEX)
31.3.12	Group Separator	F	GS	1	C_1	1D (HEX)
31.3.14	Group Separator	F	GS	1	C_1	1D (HEX)
31.3.16	Group Separator	F	GS	1	C_1	1D (HEX)
31.3.18	Group Separator	F	GS	1	C_1	1D (HEX)
31.3.19	SCA Exemption Indicator (see Note 4)	F	H	4	M	See Table 14 of ASTS SCA Exemption Indicator **MIT transaction:0100** **Recurring Payment: 0200**

Note 4: A Recurring Payment SCA Exemption Indicator is to be used when the transactions will all be for a fixed amount. Variable amount transactions should use the MIT transactions SCA Exemption Indicator.

Appendix B – Settlement Sub-Records

All stored credential authorisations require specific flags in Sub-Record Format Type 01 (General Sub-Record). **Subsequent MIT transactions only require the SCA exemption flags setting in Sub-Record Format Type 41 (3D Secure Sub-Record) under specific circumstances explained below**. (**NOTE: This is a change from previous versions of the document and earlier versions of the ASTS)**

Stored Credential Flags

Type 01: General Sub-Record

Num	Name	POS	Type	Len	Value
1	Sub-Record Counter	0	N	4	The sequence of the sub-record in relation to all sub-records submitted for this transaction starting at '0001' and up to the value sent in the 'Sub-Record Count' field sent in Segment 2
2	Reserved For Future Use	+4	A	15	Space Filled
3	Transaction Code	+19	N	2	'01'
4	Reserved For Future Use	+21	A	4	Space Filled
5	POI Capabilities	+25	A	24	
6	Payment Attributes	+49	A	24	See table below
7	Reserved for future use	+73	A	10	Space Filled
8	Record Sequence Number	+83	N	7	The sequence number of this record within the file.
90 Byte Record.					

Payment Attributes Data Values (to Be Used with Field 6)

Values used in this table should remain consistent with the Customer Instruction Value used.

POS	Attribute	Value	Meaning
1	Card Acceptor/Cardholder Agreement (see Note 1)	C	Unscheduled Payment
		I	Instalment
		N	Not Applicable
		R	Recurring Payment
2	Cardholder Not Present Condition (see Note 2)	C	Cardholder Not Present (unspecified)
		M	Mail Order
		N	Not Applicable (i.e. cardholder present)
		T	Telephone Order
		E	Electronic Commerce

POS	Attribute	Value	Meaning
3	Debt Repayment Indicator (see Note 3)	D	Debt Repayment
		N	Not Applicable
4	Stored Payment Details Indicator	F	Payment Details Stored for First Time
		N	Not Applicable
		S	Using Previously Stored Payment Details
5	Reserved For UK Finance		
6	,,,		
24	Reserved For UK Finance		

Note 1: Values other than N only to be used with cardholder present, cardholder not present, continuous authority or electronic commerce sale message types.

Note 2: If the Customer Instruction Value = 2 then the correct value for this position is 'C'

Note 3: The default value of this field is 'N'. The value 'D' is restricted to specific merchant categories and should only be used after consultation with Global Payments.

SCA and SCA Exemption Flags

Type 41: 3D Secure Sub-Record

Please note, unfortunately advice on the use of the sub-record type is subject to change as the card scheme rules evolve.

This sub-record must be populated:

- For all Customer Initiated Transactions when 3DS was performed. These transactions will be supported by a CAV in #6
- For all SCA exempted transactions (Merchant or Customer Initiated Transaction) when the issuer ACS was consulted and a cryptogram was issued to approve the exemption.
- For all Mastercard MITs performed with a stored token PAN. (These transactions will not have a CAV in #6)

This sub-record is not required:

- For all any 'straight to authorisation' SCA exempted transactions performed with a card PAN (and there is no CAV to populate in #6)
- For CITs made with an in-app token wallet.
- Visa MIT transactions whether performed with a card PAN or a token PAN if no CAV is available.

Num	Name	POS	Type	Len	Value
1	Sub-Record Counter	0	N	4	The sequence of the sub-record in relation to all sub-records submitted for this transaction starting at '0001' and up to the value sent in the 'Sub-Record Count' sent in Segment 2
2	3D Secure Program Protocol	+4	N	2	'00'= No 3DS – SCA Exempted. '01' = 3D Secure 1.x '02'= 3D Secure 2.x
3	Customer Instruction Modifier	+6	N	3	See **Table 17** for possible values
4	Reserved For Future Use	+9	A	10	Space Filled
5	Transaction Code	+19	N	2	'41'
6	Cardholder Authentication Value	+21	A	48	The result of the 3DS Secure authentication (UCAF or CAVV) as an alphanumeric string left justified and padded with spaces. This value should be populated for SCA exempted transactions when a cryptogram was returned from the ACS.
7	Reserved For Future Use	+69	A	14	Space Filled
8	Record Sequence Number	+83	N	7	Sequence number of this record within the file
9	Directory Server Transaction ID	+90	A	36	The value supplied by the 3D Secure Server. Space filled if not applicable
126 Byte Record					

Table 17 Customer Instruction Modifier Values

This table lists the correct use for the Customer Instruction Modifier Value in Sub-Record Format Type 41

The Customer Instruction Modifier should not be used for split shipments unless in very specific circumstances.

The default value for the Customer Instruction Modifier field is '000'.

- '217' should only be used for subsequent Credential on File transactions secured with a 3Ri cryptogram in # 6 and when the Mastercard ECI value was 7
- '216' should only be used when an Acquirer SCA Exemption was requested and approved by the Issuer ACS and secured by a cryptogram in # 6 and when the Mastercard ECI value was 6.

Value	Description\Use
000	Default value. All transactions when 3DS Secure took place and the cardholder was authenticated.
216	SCA Exempted Transaction supported by a CAV in #6
217	Recurring transaction supported by a CAV in #6 (3Ri transaction)
246	Mastercard token wallet MIT transaction (variable amount)
247	Mastercard token wallet MIT transaction (fixed amount Recurring Transaction)

Appendix C – Example Combinations of Payment Attributes Settings by Transaction Type

This section provides examples of the correct data values for some of the transaction types. Not all transaction types are listed. Appendix A and Appendix B contain the data values for all the transaction types.

Cardholder Initiated Transactions

Storing Cardholders Credentials for the First Time

The first transaction must be subject to SCA, whether 3D Secure for ecommerce or chip and PIN for face to face transactions. An SCA exemption must not be requested.

A transaction authorisation request message must be populated as follows:

- **Ecommerce Sale Transaction[1]** – the transaction must include the authorisation request message formatted as detailed in the *ASTS Guide,* together with the Ecommerce Auxiliary Data Record, and the Payment Attributes Auxiliary Data Record set to:
  - **Position 1** of the Payment Attributes set to **'C'**,
  - **Position 2** of the Payment Attributes set to **'E'**, and
  - **Position 4** of the Payment Attributes set to **'F'**.
- **Ecommerce Pre-authorisation Transaction[1]** – (for example, when a cardholder's registering with a hotel and booking an initial stay), the transaction must include the authorisation request message formatted as detailed in the *ASTS Guide,* together with the Authorisation Status set to **'E'**; the Ecommerce Auxiliary Data Record, and the Payment Attributes Auxiliary Data Record set to:
  - **Position 1** of the Payment Attributes set to **'C'**,
  - **Position 2** of the Payment Attributes set to **'E'**, and
  - **Position 4** of the Payment Attributes set to **'F'**.
- **Ecommerce Account Verification Transaction[1]** – (for example, when a cardholder's signing up for a magazine subscription that's not due to start until sometime in the future) the transaction must include the authorisation request message formatted as detailed in the *ASTS Guide,* together with the message type set to **'Account Verification'**, the Transaction Amount set to **'zero'**, the Ecommerce Auxiliary Data Record, and the Payment Attributes Auxiliary Data Record set to:
  - **Position 1** of the Payment Attributes set to **'C'**,
  - **Position 2** of the Payment Attributes set to **'E'**, and
  - **Position 4** of the Payment Attributes set to **'F'**.

[1]For all of the above examples, the Scheme Reference Data from the authorisation must be retained for use with subsequent transactions performed as Merchant Initiated Transactions using the stored credentials.

Using Previously Stored Cardholder Credentials

Subsequent transactions must be subject to SCA unless an SCA exemption is invoked.

A transaction authorisation request message must be populated as follows:

- **Ecommerce Sale Transaction[2]** – the transaction must include the authorisation request message formatted as detailed in the *ASTS Guide,* together with the Ecommerce Auxiliary Data Record, and the Payment Attributes Auxiliary Data Record set to:
  - **Position 1** of the Payment Attributes set to **'N'**,
  - **Position 2** of the Payment Attributes set to **'E'**, and
  - **Position 4** of the Payment Attributes set to **'S'**.
- **Ecommerce Pre-authorisation Transaction[2]** – (for example, when a cardholder's booking a stay at a hotel that they've already registered with and stored their credentials for), the transaction must include the authorisation request message formatted as detailed in the *ASTS Guide* together with the Authorisation Status set to **'E'**; the Ecommerce Auxiliary Data Record, and the Payment Attributes Auxiliary Data Record set to:
  - **Position 1** of the Payment Attributes set to **'N'**,
  - **Position 2** of the Payment Attributes set to **'E'**, and
  - **Position 4** of the Payment Attributes set to **'S'**.

[2]The transaction authorisation request message may optionally also include Auxiliary Data Record Type 10 – Authorisation Network Reference Data containing the Scheme Reference Data from the transaction that originally stored the cardholder's credentials.

Merchant Initiated Transactions

Merchant Initiated Transactions (MITs) can only follow a Customer Initiated Transaction (CIT) and so there will not be MITs when position 4 of the Payment Attributes is set to 'F'

Merchant Initiated Transactions should have position 2 set to '**C**' in settlement when the Customer Instruction value = 2

Standing Instructions – Transactions Being Performed Using Stored Credentials

- **Recurring Payment[3] –** The transaction must include the authorisation request message formatted as detailed in the *ASTS Guide*, together with any required Auxiliary Data Records, and the Payment Attributes Auxiliary Data Record set to:
  - **Position 1** of the Payment Attributes set to **'R'**,
  - **Position 2** of the Payment Attributes set to the appropriate data value for the way the transaction is being processed, and
  - **Position 4** of the Payment Attributes set to **'S'**.
- **Instalment Payment[3] –** The transaction must include the authorisation request message formatted as detailed in the *ASTS Guide*, together with any required Auxiliary Data Records, and the Payment Attributes Auxiliary Data Record set to:
  - **Position 1** of the Payment Attributes set to **'I'**,
  - **Position 2** of the Payment Attributes set to the appropriate data value for the way the transaction is being processed, and
  - **Position 4** of the Payment Attributes set to **'S'**.
- **Unscheduled Credential on File Transaction[3] –** The transaction must include the authorisation request message formatted as detailed in the *ASTS Guide*, together with any required Auxiliary Data Records, and the Payment Attributes Auxiliary Data Record set to:
  - **Position 1** of the Payment Attributes set to **'C'**,
  - **Position 2** of the Payment Attributes set to the appropriate data value for the way the transaction is being processed, and
  - **Position 4** of the Payment Attributes set to **'S'**.

  [3]For all these transaction types, the transaction authorisation request message must also include Auxiliary Data Record Type 10 – Authorisation Network Reference Data containing the Scheme Reference Data from the transaction that originally stored the cardholder's credentials.

Industry Practices – Transactions Being Performed Using Previously Stored Credentials

To avoid card issuers requesting SCA, an appropriate SCA exemption should be requested.

- **Incremental Authorisation[2]** – The transaction must include the authorisation request message formatted as detailed in the *ASTS Guide*, together with the Authorisation Status set to '**E**; any appropriate Auxiliary Data Record, and the Payment Attributes Auxiliary Data Record set to:
  - **Position 1** of the Payment Attributes set to **'L'**,
  - **Position 2** of the Payment Attributes set to the appropriate data value for the way the transaction is being processed, and
  - **Position 4** of the Payment Attributes set to **'S'**.

  Note: Incremental Authorisations are only permitted for merchants in certain categories (Merchant Category Codes). Please check with your Relationship Manager before using this transaction type.

- **Resubmission[2]** – The transaction must include the authorisation request message formatted as detailed in the *ASTS Guide*, together with any appropriate Auxiliary Data Record, and the Payment Attributes Auxiliary Data Record set to:
  - **Position 1** of the Payment Attributes set to **'S'**,

    - **Position 2** of the Payment Attributes set to the appropriate data value for the way the transaction is being processed, and
    - **Position 4** of the Payment Attributes set to **'S'**.
- **Reauthorisation[2]** – The transaction must include the authorisation request message formatted as detailed in the *ASTS Guide*, together with any appropriate Auxiliary Data Record, and the Payment Attributes Auxiliary Data Record set to:
    - **Position 1** of the Payment Attributes set to **'A'**,
    - **Position 2** of the Payment Attributes set to the appropriate data value for the way the transaction is being processed, and
    - **Position 4** of the Payment Attributes set to **'S'**.
- **Delayed Charges[2]** – The transaction must include the authorisation request message formatted as detailed in the *ASTS Guide*, together with any appropriate Auxiliary Data Record, and the Payment Attributes Auxiliary Data Record set to:
    - **Position 1** of the Payment Attributes set to **'D'**,
    - **Position 2** of the Payment Attributes set to the appropriate data value for the way the transaction is being processed, and
    - **Position 4** of the Payment Attributes set to **'S'**.
- **No Show[2]** – The transaction must include the authorisation request message formatted as detailed in the *ASTS Guide*, together with any appropriate Auxiliary Data Record, and the Payment Attributes Auxiliary Data Record set to:
    - **Position 1** of the Payment Attributes set to **'X'**,
    - **Position 2** of the Payment Attributes set to the appropriate data value for the way the transaction is being processed, and
    - **Position 4** of the Payment Attributes set to **'S'**.

[2]The transaction authorisation request message must also include Auxiliary Data Record Type 10 – Authorisation Network Reference Data containing the Scheme Reference Data from the transaction that originally stored the cardholder's credentials.

Lines are open between 9am - 6pm Monday to Friday, excluding public holidays. If you have a speech or hearing impairment, you can call us using the Relay Service by dialing 18001 followed by 0345 702 3344. Calls may be recorded. To help us continually improve on our service and in the interests of security, we may monitor and/or record your telephone calls with us. Any recordings remain our sole property.

Appendix D – Transactions performed with tokenised PANS

This section provides guidance for transactions performed using tokens.

There are two types of tokens to consider:

- Those stored in third party wallets such as Apple Pay and Google Pay
- Those requested by the merchant for a specific purpose so called 'Card on File tokens'. These are unique to the merchant and may be used for CITs or MITs. CITs performed with a token will still require SCA under PSD2 although this may be through delegated authentication methods rather than relying on 3DS.

Rules on use.

> Visa does not permit a merchant to store tokens held in third party wallets for subsequent MITs unless the original transaction was performed face to face and the MIT transaction is an Industry Practice transaction**. Stored third party wallet tokens of Visa cards may not be captured by any means for future use in a standing instruction MIT.**
>
> Mastercard permits stored tokens to be captured in-app for future use as any MIT
>
> Both Visa and Mastercard encourage merchants to request the card used in the original CIT to be tokenized (by the card scheme) and stored as a token rather than a PAN for future Industry Practice MITs.

It is also worth noting that even if the token wallet is stored on a mobile phone device it is not a MOTO transaction

Cardholder Initiated Transactions

Authorisation

The first transaction must be subject to SCA, which for in-app token wallets will depend on the wallet and the device. The wallet will provide a cryptogram and an ECI value.

Visa in-app token wallet transactions should use authorization Auxiliary Data Record Type 0101.
Mastercard in-app token wallet transactions should use Auxiliary Data Record Type 0102.

> The correct cryptogram must be submitted in the correct field specified in the ASTS.
>
> Visa has now confirmed that an ECI value of 5 is now permitted if accompanying a TAVV.
>
> ATSD. - Please note the footnote in the ASTS to Table 9 that reminds that "In-app token wallets authenticated by the token wallet and guaranteed with a cryptogram should be flagged as if the appropriate 3DS authentication had been carried out in positions 3 and 4."

Auxiliary Data Record Type 18 - Payment Attributes. - Customer initiated in-app token wallet transactions should be treated as e-commerce so:

- **Position 1** of the Payment Attributes set to **'C'**,
- **Position 2** of the Payment Attributes set to **'E'**, and
- **Position 4** of the Payment Attributes set to **'F'**.

As always the Scheme Reference Data must be requested and must be retained from the authorisation response for use with subsequent transactions performed as Merchant Initiated Transactions using the stored credentials.

If the transaction is approved, then the tokenized PAN may be stored to be used for future CITs and or MITs (subject to the rules above).

Subsequent Customer Initiated Transactions using a COF scheme token still require SCA to be performed. A Mastercard COF token when authenticated by a non 3DS method will produce a V3 cryptogram. In order that dynamic linking can be performed in compliance with PSD2 regulation the Card Acceptor Identifier must be submitted using Auxiliary Data Record Type 0103 in addition to Auxiliary Data Record Type 0102. Visa does not have this requirement.

Settlement

As noted under the text of Segment 1 in the ASTS with regards to the Customer Instruction Value.

The value of Y should only be used when the in-app payment was made using authorisation auxiliary data-record 0102 and a cryptogram was submitted in position 31.3.7. That is a secure in-app transaction performed with a Mastercard stored credential in a token wallet device. All other token wallet transactions should use the appropriate Ecommerce/Continuous Authority value.

For a Visa in-app token wallet CIT use a CIV of G.
For a Mastercard in-app token wallet CIT use a CIV of Y.

Sub-record Format Type 1 is required and the Payments attributes should match those of the authorization.
Sub-record Format Type 2 is optional if the values are known. It is not necessary to send an empty record.
Sub-record Format Type 41 is not required unless 3DS took place.

Merchant Initiated Transactions

As with all MIT transactions whether performed with a card PAN or a token PAN, these are continuous authority transaction types and not e-commerce. All values submitted should be consistent with that definition.

Authorisation

The message type must be a continuous authority one such as ‘A0’.

These transactions need to be noted with one of the two MIT SCA exemptions.

A MIT performed with a stored Visa token should use Auxiliary Data Record Type 0101.
A MIT performed with a stored Mastercard token should use Auxiliary Data Record Type 0102.

The appropriate SCA exemption flag should be used.

Auxiliary Data Record Type 18, Payment Attributes. – Merchant initiated transactions performed with a token PAN are no different to any other MIT so:

- **Position 1** of the Payment Attributes set to an appropriate value e.g. **‘C’ ‘I’ or ’R’**,
- **Position 2** of the Payment Attributes set to **‘C’**, and
- **Position 4** of the Payment Attributes set to **‘S’**.

Position 2 should not be ‘E’ because this is not an e-commerce transaction.

Auxiliary Data Record Type 26 MUST be present and populated with the Scheme Reference Data from the original CIT.

Settlement

The correct Customer Instruction Value for a continuous authority transaction in Segment 1 is ‘2’.

Sub-record Format Type 1 is required and the Payment Attributes should match those of the authorisation.

Sub-record Format Type 41 is required for Mastercard transactions. Specifically, the Customer Instruction Modifier must be set to one of two values. ‘246’ or ‘247’. (See Appendix B above)