Global Payments

Stored Credential Technical Implementation Guide V2.0

April 2022

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
2.0	Rewrite	01/06/2022	Rewrite with substantive changes following introduction new Mastercard requirements and addition of new fields and values in S70	Schemes Consultancy	Testing & Schemes

Contents

1. Introduction and document scope

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. These rules and specifications have been modified multiple times since original implementation, primarily to allow the card schemes to remain compliant with the Payment Services Directive 2 (PSD2, below). The rules and specifications are collectively known as the Stored Credential Framework.

For clarity the scope of the Stored Credentials Framework explained in this document is when a merchant or their agent stores the credentials for exclusive use with that merchant (by either the merchant or the cardholder). A transaction being made by a card holder using a token wallet, such as Apple Pay or Google Pay is not automatically a stored credential transaction in the context of the framework because it is the third party wallet and not the merchant or its agent that has stored the credentials.

The context of this document is a transaction being performed by a UK based merchant. Definitions and rules used in this document are those pertaining to a UK based merchant with a UK based acquirer.

This document explains the specific data values (including the 'Stored Credential Indicators' within the Payment Attributes field) defined within Standard 70 used by Global Payments to meet the requirements of 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 https://www.globalpayments.com/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 was delayed in the UK until March 2022, 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.

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.

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.

Both follow an initial Customer Initiated Transaction, which must meet specific criteria before a stored credential transaction.

2.1 Initial Customer Initiated Transactions- used to store credentials

A Customer or 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. PSD2 requires that unless the transaction is out of scope for SCA, the card holder must be authenticated and the transaction approved before the credentials are stored.

- Card present transactions must use chip and PIN. A contactless transaction made with a card is not subject to SCA and so cannot be used within the stored credential framework.
- MOTO (Mail Order\Telephone Order) transactions are out of scope for SCA so may be used within the stored credentials framework, providing that the transaction is approved.
- E-commerce transactions must be subject to SCA. In order for this to happen the authentication request must contain the 'challenge flag' to ensure that cardholder is not passively authenticated. This requires the use of EMV 3DS (3DS v2) because 3DS v1 does not contain that functionality.
- An Account Verification Message (also known as a £0 Auth) may be used to initiate the stored credential framework, but it should follow a 3DS v2 authentication (as per an Ecommerce transaction) for a typical amount that is expected to follow. For example, if the customer will be billed a recurring amount of £50 after 3 months, authentication should take place for £50 at the time of the account being created with the AVM.

2.2 Customer Initiated Credential on File Transactions

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 because the merchant uses the card details previously stored by the cardholder to perform the transaction.

These transactions will primarily be Ecommerce or in-app. All e-commerce CITs are subject to SCA requirements, even those made with stored credentials and should be authenticated with 3D Secure, or a suitable SCA exemption flag (such as 'low value'). Because the transactions are authenticated it is not necessary to submit the SRD to allow an issuer to connect back to the previously approved transaction.

It is possible that these transactions could be MOTO, the merchant has stored the card holder's credentials for future phone calls. In this scenario the transaction should be clearly marked as a MOTO transaction (using the correct transaction type etc.).

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

2.3 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.

A MIT transaction is generally not secure (because the merchant has requested an exemption) and the merchant takes liability for such transactions. A framework does exist whereby a merchant can perform a 3RI transaction (a form of customer not present SCA using 3DS V2.2 or above.) If the transaction is authenticated, then the issuer takes liability. This framework is still in its infancy and not widely supported yet. For more details of 3RI transactions see the Global Payments PSD2 and SCA Technical Implementation Guide.

The issuer is able to approve the unsecure MIT authorisation request because it contains the Scheme Reference Data (SRD) from the original CIT approval response which ties the subsequent MIT back to the authenticated CIT.

NOTE
To support the implementation of the Stored Credential Framework and the transition to PSD2, the card schemes supplied acquirers with a 'dummy' SRD that they could insert into the authorisation message on behalf of their merchant if for some reason the merchant had not been able to store it from the original CIT. Permission to use the dummy value was extended twice, but Visa will not permit the use of a dummy SRD from October 2022 and backdate usage fines to August 2022 for merchants not populating the SRD correctly in the MIT authorisation request. As a result, Global Payments will cease to populate the SRD value before October 2022. Merchants and their PSPs must have a solution in place ahead of this time because MIT transactions without SRD in them will be declined by issuers.

MITs can be split into two kinds of transactions:

- Standing Instructions
- Industry Practices

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 or variable pre agreed amount. Recurring Transactions don't have a fixed duration and will continue to be processed until the cardholder cancels the agreement. **Note** that the definition of 'recurring payment' is slightly different in the context of an SCA Exemption. (See **Appendix A**, SCA Exemption Flags)
- **Instalment Payments –** transactions that are processed on a regular fixed interval for a known pre agreed amount for a single purchase. 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.

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.

2.4 Starting a new merchant agreement with previously stored credentials.

Once a cardholder has been authenticated and agreed to allow a merchant to store their payment credentials, the credentials can be used to initiate multiple agreements without the need to perform SCA again.

For example, if a cardholder takes out an insurance policy costing £120 with a provider and agrees to pay monthly, at the time of the first payment the cardholder performs a (secure) CIT for £10 and the issuer then subsequently takes 11 more payments for £10 as MITs. After the year is over the card holder chooses to renew the policy for a new annual price of £132. In month 13 the merchant (if they wish) can simply perform a MIT for £11 to start the new agreement rather than subject the card holder to SCA and a new agreement.

Standard 70 has introduced a new value in position 11 of the authorisation Payment Attributes to indicate clearly when this is happening.

2.5 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 e-commerce 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.

2.6 Other tokenized transactions

Merchants together with their PSPs may choose to tokenize 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 authorisation. See the ASTS for details. CITs are still subject to SCA even those performed with stored PANS.

2.7 Other notable transaction types

Refund Transactions

Refund transactions are outside of the scope of the stored credential framework and should not be flagged as such even if the original sale was made as either a MIT or a CIT with stored credentials.

Account Verification Transactions as MITs

When a customer creates an account with a merchant but does not yet wish to purchase anything (or there may be an initial introductory 'free period' before a merchant takes a payment) the credentials may be stored based on an AVT (as above in Section 2.1). If merchant wishes to check whether an account is still valid before taking a MIT payment it may perform a non-secure AVS transaction (for £0). Visa card scheme rules do not permit this to be flagged as a stored credential transaction.

Global Payments does not recommend the use of AVT transactions in this way, (use of our Recurring Transaction Enquiry Service provides more helpful information) but merchants wishing to do this are advised that the transactions should simply be flagged as an AVT without Payment Attributes to prevent confusion.

Mastercard Pre-Auths and Final Auths

Mastercard has the concept of a 'Pre-Authorisation' message request which can then be modified by a 'Final' authorisation message. In an e-commerce environment the final authorisation will usually be a MIT. Mastercard does not consider that a merchant storing cardholder details to simply complete a standalone single transaction is acting within the stored credentials framework.
This means that even though the final authorisation is a MIT and requires all the correct MIT flags in the authorisation message and the SRD from the pre-authorisation to tie the two together, it is not necessary to set Stored Payment Details Indicator in the Payment Attributes.

If the Pre-authorisation transaction is being performed with both the intent that there will be a subsequent Final Authorisation and the merchant is going to store the card holder credentials for future transactions as well, then it is necessary to set Stored Payment Details Indicator in the Payment Attributes

Visa Incremental Transactions

Visa does not have the concept of pre-auths and final auths and supports the specific transaction type of 'incremental authorisation' within the stored credential framework. Stored Credential Indicators in the Payment Attributes should be set to perform incremental authorisations with a Visa card product.

2.8 Other Merchant Initiated Transactions.

As stated above (in the Mastercard Pre-Auths and Final Auths section) not all MITS fall within the stored credential framework. If the transaction is a single standalone transaction
However all MIT authorisations MUST:

- Be Message Type 'A0/A1'
- Have an appropriate SCA exemption flag set
- Have the Scheme Reference Data from the original CIT
- Have payment Attributes Position 1 (Card Acceptor/Cardholder Agreement) set to an appropriate value to indicate what kind of MIT it is.

.

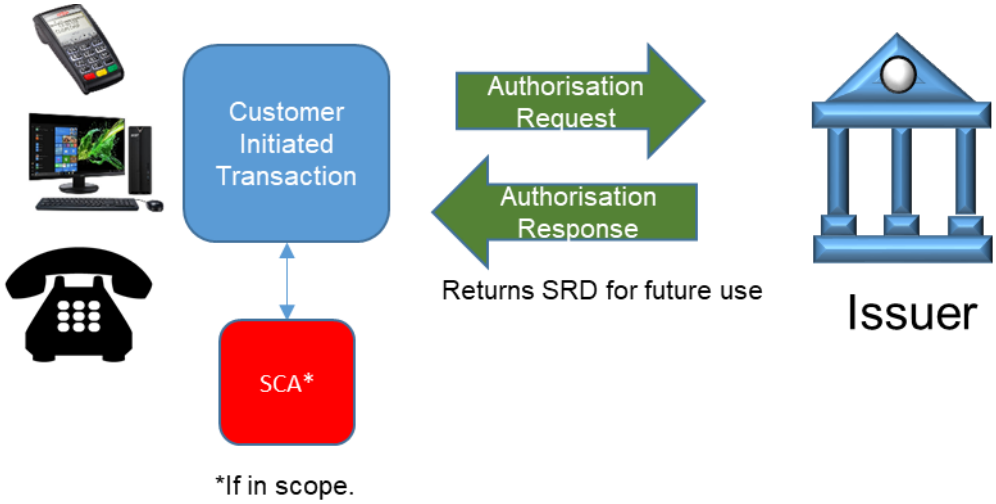
3. Technical Requirements for Credential on File Transactions

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 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. This will require the use of 3DSv2 with a challenge flag set to ensure that the issuer actually authenticates the card holder

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 requested, 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).

Key data fields in authorisation.

- Message type must accurately reflect the nature of the transaction e.g. '09' for MOTO or 'B2' for E-com
- Additional Data Record Type 0101 with full 3DSv2 data is required for E-com transactions
- Additional Data Record Type 18 carries the stored credential flags as Payment Attributes. In the initial transaction:
    - Position 1 should be 'C', 'I' or 'R' depending on the reason the credentials are being stored.
    - Position 2 should match the message type
    - Position 3 should be set as appropriate.'
    - Position 4 MUST be 'F'
    - Positions 5 to 10 can be spaced filled
    - Position 11 MUST be 'N'
    - Position 12 should be set to appropriate value

See Appendix A for the full specification of the authorisation auxiliary data records.
See Appendix C for a set of example use cases with the expected values.

Key data fields in settlement.

- The Customer Instruction Value (CIV) in Segment 1 must match that of the original authorisation. e.g. '01' for MOTO or 'G2' for authenticated E-com
- Sub-Record Format Type 41 with full 3DSv2 data is required for E-com transactions
- Sub-Record Format Type 01 carries the stored credential flags. These should match the values submitted in authorisation. In the initial transaction:
    - Position 1 should be 'C', 'I' or 'R' depending on the reason the credentials are being stored.
    - Position 2 should match the message type (either 'T' or 'M' may be used if a PSP has no way to distinguish between them)
    - Position 3 should be set as appropriate. 'N' is default
    - Position 4 MUST be 'F'
    - Positions 5 onwards should be spaced filled

See Appendix B for the full specification of the settlement sub-records.

3.2 Performing Customer Initiated Transactions Using Stored Credentials

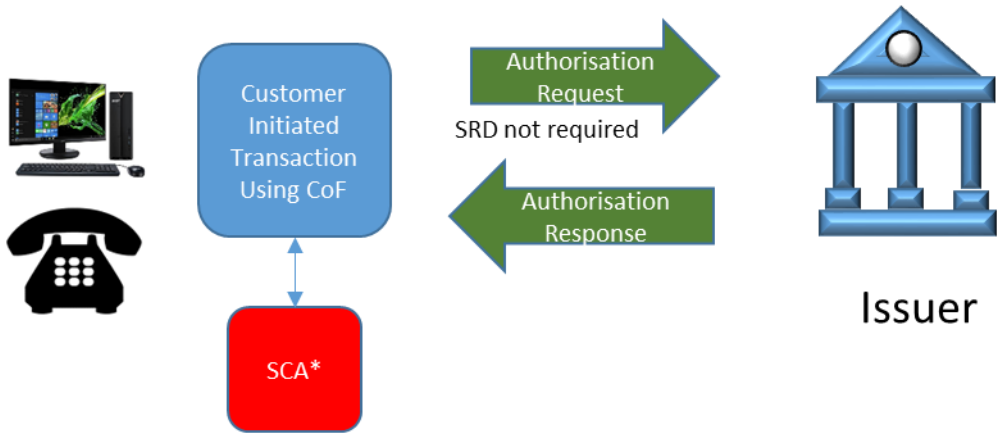
A card holder can store their credentials with a merchant for mutual convenience when making future purchases. In the UK because PSD2 requires SCA and a card needs to be inserted for off-line PIN validation, this renders the storing of credentials in a customer present environment pointless. Card holder details can only really be stored for cardholder not present use cases. The primary use case being Ecommerce.

Storing credentials for future Ecommerce CITs does not absolve the merchant from performing SCA (or requesting an SCA exemption). The only difference in the authorisation message between an E-commerce transaction performed with stored credentials and one when a card holder entered their details at the time of the transaction are the mandatory presence of Payment Attribute flags.

Scheme Reference Data from the initial transaction is not required because SCA has been performed.

The second use case for customer initiated subsequent transactions is MOTO. Using stored credentials means that the card holder does not need to repeat personal information aloud down the phone for a second time.

This transaction is a still a MOTO transaction and must be unambiguously flagged as so.



* If in scope, an exemption may be used

<u>Key data fields in authorisation.</u>

- Message type must accurately reflect the nature of the transaction e.g. '09' for MOTO or 'B2' for E-com
- Additional Data Record Type 0101 with full 3DSv2 data is required for E-com transactions
- Additional Data Record Type 18 carries the stored credential flags as Payment Attributes. In the subsequent CIT transaction:
    - Position 1 should be 'N' – there is no payment agreement for ad-hoc CITs
    - Position 2 should be either 'M' or 'T' or 'E'
    - Position 3 should be set as appropriate. 'N' is default'
    - Position 4 MUST be 'S'
    - Positions 5 onwards can be spaced filled

See Appendix A for the full specification of the authorisation auxiliary data records.
See Appendix C for a set of example use cases with the expected values.

<u>Key data fields in settlement.</u>

- The Customer Instruction Value in Segment 1 must match that of the original authorisation. e.g. '01' for MOTO or 'G2' for authenticated E-com
- Sub-Record Format Type 41 with full 3DSv2 data is required for E-com transactions
- Sub-Record Format Type 01 carries the stored credential flags. These should match the values submitted in authorisation
    - Position 4 MUST be 'S'
    - Positions 5 onwards should be spaced filled

See Appendix B for the full specification of the settlement sub-records.

3.3 Performing Merchant Initiated Transactions Using Stored Credentials

Merchant Initiated Transactions (as defined in Section 2.3) are always subsequent transactions which follow a Customer Initiated Transaction which included a customer agreement that gave the merchant permission to initiate transactions in specific circumstances.

It is important to note that MITs are not ecommerce transactions and should not be flagged as such in either the authorisation or the settlement message. It is unfortunate and confusing that the SCA exemption indicators required by schemes were added to the Standard 70 Ecommerce message blocks in both authorisation and settlement but the transactions 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.

There are two possible SCA exemption flags that can be used. If the transaction amount can vary then use the MIT exemption indicator (value '0100'). If the transaction amount will be a fixed amount then use the Recurring Payment exemption indicator (value 0200). Position 12 in the Payment Attributes should match this value.

In authorisation the message type used should be '0A' 'Continuous Authority' and in settlement the Customer Instruction Value in Segment 1 must be '2' Continuous Authority for all MITs.

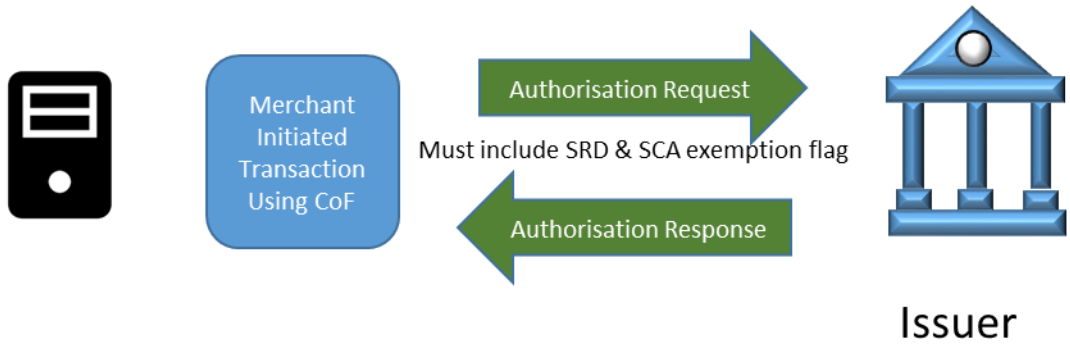
If the Customer Instruction Value is '2' – Continuous Authority, then the second position of the Payment Attributes (Table 12 of the ASTS) is 'C' cardholder not present (unspecified). It should never be 'E' or 'N' when the Customer Instruction value is '2'

Scheme Reference Data from the original authorisation (or a previously approved MIT transaction in the chain if the original is not available for historic reasons) is submitted in the authorisation request to allow the card issuer to tie the current non-secure MIT transaction back to original CIT that was subject to SCA.

The Scheme Reference Data submitted in the settlement record should be that returned in the associated authorisation response to allow the card issuer to match the settlement record with the authorised amount before adding it to the cardholder's statement.

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

MIT transactions incorrectly formatted and lacking SRD and an explicit SCA Exemption Indicator will likely be declined by card issuers with an 'SCA Required' decline reason.



Key data fields in authorisation.

- Message type must be ‘A0/A1’
- Additional Data Record Type 0101 with an appropriate SCA exemption indicator is required.
- Additional Data Record Type 10 is required to carry the SRD
- Additional Data Record Type 18 carries the stored credential flags as Payment Attributes. For MIT transaction:
    - Position 1 MUST NOT be ‘N’. If the initial CIT was ‘I’ or ‘R’ it should be the same in the following MITs.
    - Position 2 MUST BE ‘C’ -’ Cardholder Not Present (unspecified)
    - Position 3 should be set as appropriate. ‘N’ is default’
    - Position 4 MUST be ‘S’
    - Positions 5 to 10 can be spaced filled
    - Position 11 MUST be ‘N’
    - Position 12 should be set to appropriate value that matches the SCA Exemption indicator and the value in Position 12 of the original CIT.

See Appendix A for the full specification of the authorisation auxiliary data records.
See Appendix C for a set of example use cases with the expected values.

Key data fields in settlement.

- The Customer Instruction Value in Segment 1 MUST be ‘2’.
- Sub-Record Format Type 41 is only required when a 3RI transaction was performed.
- Sub-Record Format Type 01 carries the stored credential flags. These should match the values submitted in authorisation
    - Position 1 MUST NOT be ‘N’. If the initial CIT was ‘I’ or ‘R’ it should be the same in the following MITs, otherwise use ‘C’
    - Position 2 MUST BE ‘C’ -’ Cardholder Not Present (unspecified)
    - Position 4 MUST be ‘S’
    - Positions 5 onwards should be spaced filled

See Appendix B for the full specification of the settlement sub-records.

3.4 Starting A New Customer Agreement for Merchant Initiated Transactions Using Previously Stored Credentials

This is a variation on a standard MIT (above 3.3).

All the values are the same as defined in Section 3.3, but position 11 of the Payments Attributes in the authorisation message MUST be ‘S’

When position 11 of the Payments Attributes in the authorisation message is ‘S the position 4 MUST be ‘S’’

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	Stored Payment Details Additional Information	N	Not Applicable
		S	New Agreement Made With Previously Stored Payment Details.
12	Transaction Amount Variability Indicator	F	Fixed Amount
		N	Not Applicable
		V	Variable Amount
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 (in a 3RI authentication for example) 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. Merchants\PSPs should ensure that this matches Position 12 of the Payment Attributes (above).

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 Payment Attribute data values for typical use cases. Not all transaction types are listed. Appendix A and Appendix B contain the data values for all the transaction types.

Not all required fields are illustrated below and they should be read in the context of Section 3 of this document, the Global Payments ASTS and PSD2 SCA Technical Implementation Guide.

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.

In all of the below 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.

Changes in card scheme requirements to identify even the first (customer initiated transaction) in the sequence of installment or recurring transactions means that they should be flagged as 'I' and 'R' respectively in both the MIT and CIT, although they will have different message types.

- Cardholder makes an e-commerce transaction, is authenticated and permits their card to be stored for their future use on the website.

Auth Msg Type	Auth Payment Attribute Position					SCA Exemption Indicator	Settlement CIV
	1	2	4	11	12		
B2	C	E	F	N	N	n/a	G

- Cardholder makes a telephone order, and permits their card to be stored for ease on future calls.

Auth Msg Type	Auth Payment Attribute Position					SCA Exemption Indicator	Settlement CIV
	1	2	4	11	12		
09	C	T	F	N	N	n/a	1

- Cardholder buys goods or a service online, is authenticated and permits the merchant to take regular installments for an agreed amount over a fixed period of time after the initial payment.

Auth Msg Type	Auth Payment Attribute Position					SCA Exemption Indicator	Settlement CIV
	1	2	4	11	12		
B2	I	E	F	N	N	n/a	G

- Cardholder buys goods or a service online, is authenticated and permits the merchant to take future recurring payments for a fixed amount after the initial payment.

Auth Msg Type	Auth Payment Attribute Position					SCA Exemption Indicator	Settlement CIV
	1	2	4	11	12		
B2	R	E	F	N	F	n/a	G

- Cardholder buys goods or a service online, is authenticated and permits the merchant to take future recurring payments for a variable amount after the initial payment.

Auth Msg Type	Auth Payment Attribute Position					SCA Exemption Indicator	Settlement CIV
	1	2	4	11	12		
B2	R	E	F	N	V	n/a	G

- Cardholder signs up to a website, is authenticated for a typical amount, although is not charged anything at this point, expecting that the merchant to take recurring payments at a future date. (No settlement message will be submitted because there is no purchase at this time)

Auth Msg Type	Auth Payment Attribute Position					SCA Exemption Indicator	Settlement CIV
	1	2	4	11	12		
EC	R	E	F	N	V	n/a	n\a

Using Previously Stored Cardholder Credentials

- Cardholder makes an e-commerce transaction, with their stored credentials having been authenticated via 3DS.

Auth Msg Type	Auth Payment Attribute Position					SCA Exemption Indicator	Settlement CIV
	1	2	4	11	12		
B2	N	E	S	N	N	n/a	G

- Cardholder makes an e-commerce transaction, with their stored credentials and the merchant requests a low value SCA exemption.

Auth Msg Type	Auth Payment Attribute Position					SCA Exemption Indicator	Settlement CIV
	1	2	4	11	12		
B2	N	E	S	N	N	100	J

- Cardholder makes a subsequent telephone order, with the merchant using the stored credentials for convenience and security.

Auth Msg Type	Auth Payment Attribute Position					SCA Exemption Indicator	Settlement CIV
	1	2	4	11	12		
09	N	T	S	N	N	n\a	1

- At the end of a current agreement cardholder contacts the merchant and agrees to another purchase, permitting the merchant to continue taking future recurring payments for a variable amount. This is still a CIT and must be subject to SCA with a challenge indicator to request active authentication to ensure issuers continue to accept the subsequent MITs

Auth Msg Type	Auth Payment Attribute Position					SCA Exemption Indicator	SRD required?	Settlement CIV
	1	2	4	11	12			
B2	R	E	S	S	V	n/a	N	G

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'.

Changes in card scheme requirements to identify even the first (customer initiated transaction) in the sequence of installment or recurring transactions means that they should be flagged as 'I' and 'R' respectively in both the MIT and CIT, although they will have different message types.

Standing Instructions – Transactions Being Performed Using Stored Credentials

- Merchant makes an ad-hoc payment for a variable amount transaction using cardholder's stored credentials triggered by an account balance dropping below an agreed amount.

Auth Msg Type	Auth Payment Attribute Position					SCA Exemption Indicator	SRD required?	Settlement CIV
	1	2	4	11	12			
A0	C	C	S	N	V	0100	Y	2

- Merchant makes a recurring payment for a variable amount transaction using cardholder's stored credentials.

Auth Msg Type	Auth Payment Attribute Position					SCA Exemption Indicator	SRD required?	Settlement CIV
	1	2	4	11	12			
A0	R	C	S	N	V	0100	Y	2

- Merchant makes a recurring payment for a fixed amount transaction using cardholder's stored credentials.

Auth Msg Type	Auth Payment Attribute Position					SCA Exemption Indicator	SRD required?	Settlement CIV
	1	2	4	11	12			
A0	R	C	S	N	F	0200	Y	2

- Merchant makes an installment payment for a fixed amount transaction using cardholder's stored credentials.

Auth Msg Type	Auth Payment Attribute Position					SCA Exemption Indicator	SRD required?	Settlement CIV
	1	2	4	11	12			
A0	I	C	S	N	F	0200	Y	2

Industry Practices – Transactions Being Performed Using Previously Stored Credentials

- Merchant makes an incremental authorisation transaction using cardholder's stored credentials.

Auth Msg Type	Auth Payment Attribute Position					SCA Exemption Indicator	SRD required?	Settlement CIV
	1	2	4	11	12			
A0	L	C	S	N	N	0100	Y	2

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.

- Merchant resubmits an authorisation request for reauthorisation using cardholder's stored credentials.

Auth Msg Type	Auth Payment Attribute Position					SCA Exemption Indicator	SRD required?	Settlement CIV
	1	2	4	11	12			
A0	A	C	S	N	N	0100	Y	2

- Merchant submits a delayed charge authorisation request for authorisation using cardholder's stored credentials.

Auth Msg Type	Auth Payment Attribute Position					SCA Exemption Indicator	SRD required?	Settlement CIV
	1	2	4	11	12			
A0	D	C	S	N	N	0100	Y	2

- Merchant submits a 'No Show' authorisation request for authorisation using cardholder's stored credentials.

Auth Msg Type	Auth Payment Attribute Position					SCA Exemption Indicator	SRD required?	Settlement CIV
	1	2	4	11	12			
A0	X	C	S	N	N	0100	Y	2

Appendix D – Transactions performed with tokenized 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 authorisation 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.
>
> 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 (such as Click to Pay) 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 authorisation.
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 submitted 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.
- 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.**
- Auxiliary Data Record Type 1001 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)