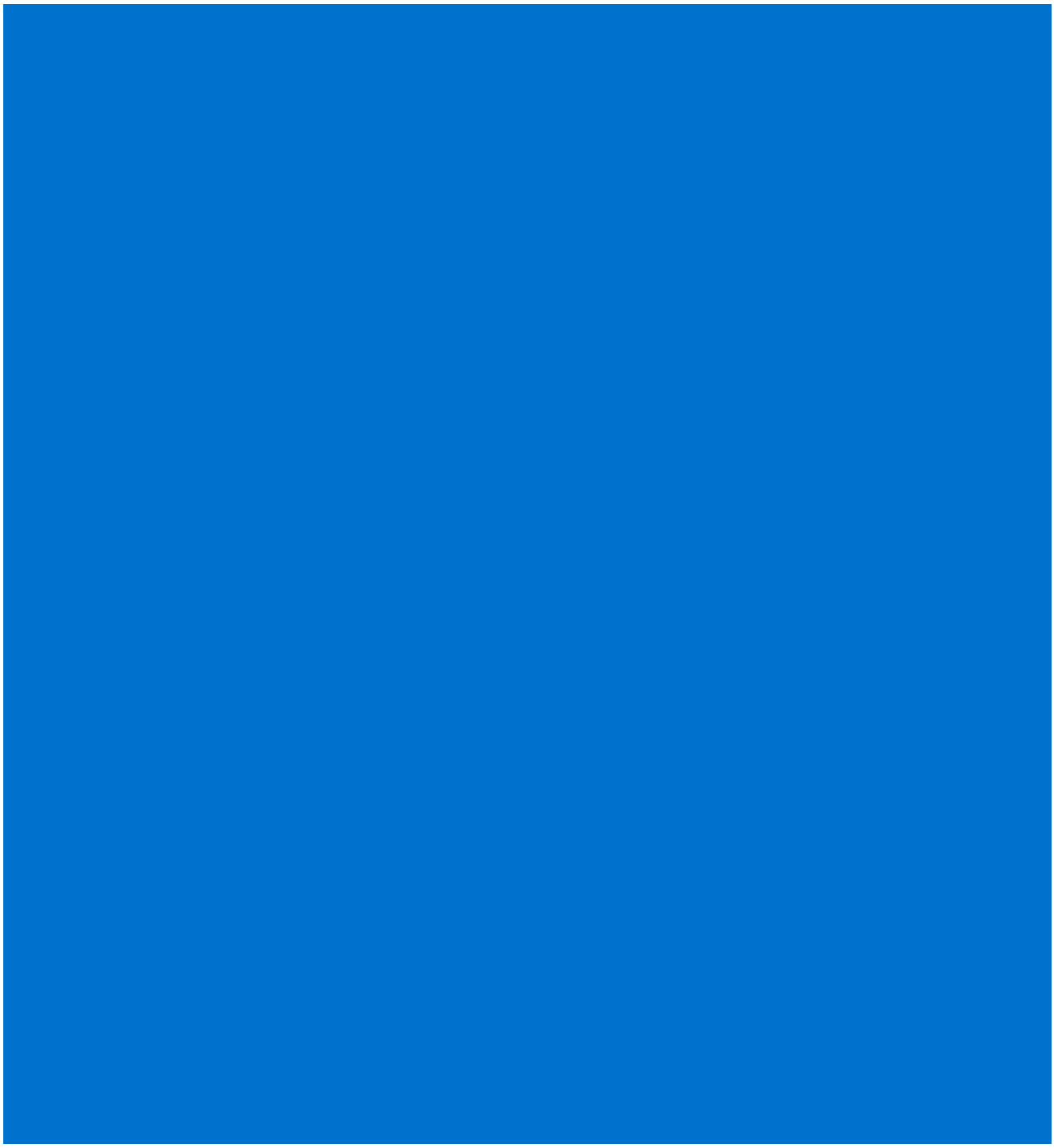
Stored Credential – Technical Implementation Guide Version 1.5



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

Contents

1. Introduction

The Card Schemes (Visa and Mastercard) 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 Visa and Mastercard 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 Visa and Mastercard, 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 can be located in the Customer Centre section of our website at **www.globalpaymentsinc.co.uk**. You'll find it within the Stored Credential Transaction option.

From **14th September 2019**, **t**he Payment Services Directive 2 has mandated that all payments will have to be validated using Strong Customer Authentication (SCA). From that date, card issuers are obliged to seek SCA or decline transactions that aren't fully authenticated that should be. It's now more critical than ever that Stored Credential Transactions are flagged correctly or the card issuer may choose to challenge the transaction and request SCA. If the cardholder can't be contacted or provide SCA, the transaction won't go ahead.

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 Customer Centre. You'll find it under the option for Strong Customer Authentication.

2. Transaction Types

This section details the transaction types that are impacted by Visa and Mastercard'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 or through a checkout online. In the 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 GPUK no longer mandates 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 give the merchant consent to store their card details, making them Credential on File MITs. This type of transaction can be split into two kinds:

- 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 amount.

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 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.

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 recommend 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 Contactless transaction,
- 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).

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 – Auxiliary Data Record). 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

When performing a transaction using a stored credential, it's important that Scheme Reference Data from the initial transaction is resubmitted 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 – Auxiliary Data Record). 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'

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 a General Sub Record, which may or may not already be part of the transaction record for other reasons.

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

Note: Payments 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.

4. 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:
    - its MOTO (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 transaction 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 CoF 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 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).

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 TraceID 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.

Appendix A – Auxiliary Data Record

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)

Posn.	Attribute	Value	Meaning
1	Card Acceptor/Cardholder Agreement	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	C	Cardholder Not Present (unspecified)
		M	Mail Order
		N	Not Applicable (i.e. cardholder present)
		T	Telephone Order
		E	Electronic Commerce
		A	Application initiated electronic commerce
3	Reserved For The UK Cards Association		
4	Stored Payment Details Indicator	F	Payment Details Stored for First Time
		N	Not Applicable
		S	Using Previously Stored Payment Details
5	Reserved For The UK Cards Association		

Posn.	Attribute	Value	Meaning
6	Reserved For The UK Cards Association		
7	Reserved For The UK Cards Association		
8	Reserved For The UK Cards Association		
9	Reserved For The UK Cards Association		
10	Reserved For The UK Cards Association		
11	Reserved For The UK Cards Association		
12	Reserved For The UK Cards Association		
13	Reserved For The UK Cards Association		
14	Reserved For The UK Cards Association		
15	Reserved For The UK Cards Association		
16	Reserved For The UK Cards Association		
17	Reserved For The UK Cards Association		
18	Reserved For The UK Cards Association		
19	Reserved For The UK Cards Association		
20	Reserved For The UK Cards Association		
21	Reserved For The UK Cards Association		
22	Reserved For The UK Cards Association		
23	Reserved For The UK Cards Association		
24	Reserved For The UK Cards Association		

Appendix B – 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)

Posn.	Attribute	Value	Meaning
1	Card Acceptor/Cardholder Agreement	C	Unscheduled Payment
		I	Instalment
		N	Not Applicable
		R	Recurring Payment
2	Cardholder Not Present Condition	C	Cardholder Not Present (unspecified)
		M	Mail Order
		N	Not Applicable (i.e. cardholder present)
		T	Telephone Order
		E	Electronic Commerce
		A	Application initiated electronic commerce
3	Reserved For The UK Cards Association		
4	Stored Payment Details Indicator	F	Payment Details Stored for First Time
		N	Not Applicable
		S	Using Previously Stored Payment Details
5	Reserved For The UK Cards Association		
6	Reserved For The UK Cards Association		
7	Reserved For The UK Cards Association		

Posn.	Attribute	Value	Meaning
8	Reserved For The UK Cards Association		
9	Reserved For The UK Cards Association		
10	Reserved For The UK Cards Association		
11	Reserved For The UK Cards Association		
12	Reserved For The UK Cards Association		
13	Reserved For The UK Cards Association		
14	Reserved For The UK Cards Association		
15	Reserved For The UK Cards Association		
16	Reserved For The UK Cards Association		
17	Reserved For The UK Cards Association		
18	Reserved For The UK Cards Association		
19	Reserved For The UK Cards Association		
20	Reserved For The UK Cards Association		
21	Reserved For The UK Cards Association		
22	Reserved For The UK Cards Association		
23	Reserved For The UK Cards Association		
24	Reserved For The UK Cards Association		

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

This section provides examples of the correct data values for some of the transactions 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

Standing Instructions – Credentials Being Stored 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.

- **Recurring Payments[1] –** 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 has been captured, and
  - **Position 4** of the Payment Attributes set to **'F'**.
- **Instalment Payments[1] –** 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 has been captured, and
  - **Position 4** of the Payment Attributes set to **'F'**.
- **Unscheduled Credential On File Transactions[1] –** 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 has been captured, and
  - **Position 4** of the Payment Attributes set to **'F'**.

[1]For all of these transactions types, the Scheme Reference Data returned in the authorisation response must be retained for submission in subsequent Merchant Initiated Transactions using the stored credential.

Standing Instructions – Transactions Being Performed Using Stored Credentials

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

- **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 transactions 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 – Credentials Being Stored 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.

- **Incremental Authorisation**[1] – 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 has been captured, and
  - **Position 4** of the Payment Attributes set to **'F'**.

  Note: Incremental Authorisations typically use cardholder credentials stored during a pre-authorisation or hotel check in. Multiple incremental authorisations may be applied to a single overall transaction to provide the merchant with sufficient authorisation protection.

  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**[1] – 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 has been captured, and
  - **Position 4** of the Payment Attributes set to **'F'**.
- **Reauthorisation**[1] – 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 has been captured, and
  - **Position 4** of the Payment Attributes set to **'F'**.
- **Delayed Charges**[1] – 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 has been captured, and
  - **Position 4** of the Payment Attributes set to **'F'**.
- **No Show**[1] – 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 has been captured, and
  - **Position 4** of the Payment Attributes set to **'F'**.

[1]All of the above transaction types must retain the Scheme Reference Data returned in the authorisation response message for resubmission during subsequent transactions.

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. 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. We also provide a Textphone service on 0345 602 4818.

Global Payments is HSBC's preferred supplier for card processing in the UK.

.