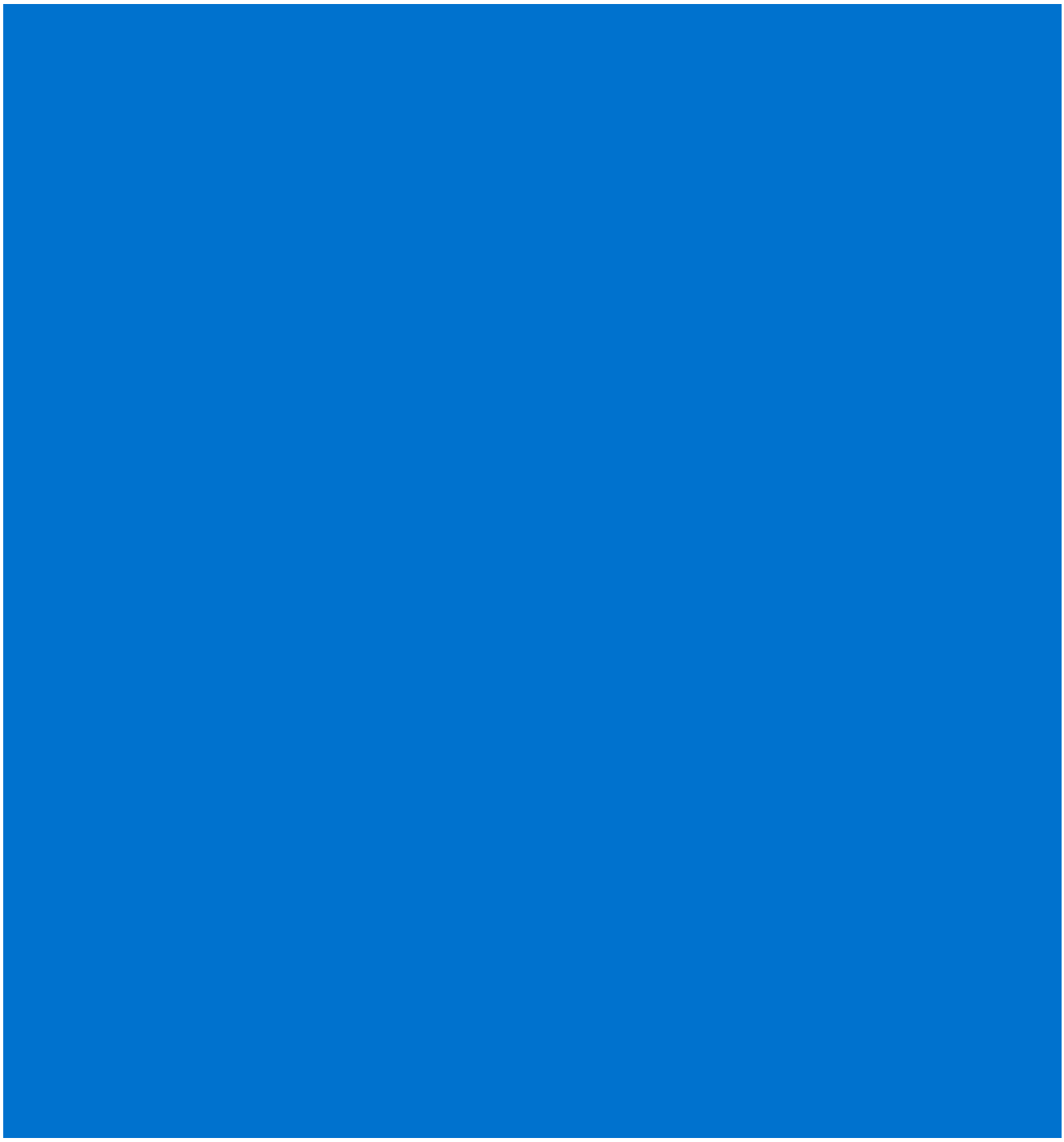
Payment Services Directive 2 and Strong Customer Authentication Technical Implementation Guide



Amendment History

Version	Status	Date Issued	Comment	Originator	Reviewed By
1.0	New	12th April 2019	Initial version issued to accompany Global Payments ASTS v1.9 April 2019 edition.	Senior Technical Consultant	Marketing
1.1	Update	1st November 2019	Update to company address only	Senior Technical Consultant	Marketing

Contents

1. Introduction

This guide provides some explanation about what the Payment Services Directive 2 (PSD2) and Strong Customer Authentication (SCA) are, and how they'll affect your business. It outlines what you need to do to be compliant with both the law and Card Scheme Rules and what changes you may need to make to your authorisation and settlement messages that you send to Global Payments.

This guide contains extracts from the Global Payments Authorisation and Settlement Technical Specification v1.9 and provides context and details to the technical changes therein.

This guide **doesn't** explain in detail, the changes and technical requirements required to implement 3D Secure changes with your Payment Service Provider (PSP). For details of those technical changes you should consult your PSP.

2. Normative References

The following documents are referenced within this guide and are essential for the application of this guide. For dated references, only the edition cited applies. For undated references, the latest version of the referenced document (including any amendments) applies.

Global Payments Authorisation and Settlement Technical Specifications (ASTS)	This guide should be read in conjunction with our full technical specifications. Compliance with version 1.9 of the ASTS is the minimum level required to support functionality outlined in this guide
UK Finance Standard 70	Card acceptor to acquirer interface standards **http://www.ukfinance.org.uk**
UK Finance guidance on the UK legal position on the implementation of PSD2	https://www.ukfinance.org.uk/guidance/uk-finance-industry-guidance-strong-customer-authentication-under-psd2
European Commission PSD2 Regulations	https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015L2366&from=EN
EBA Regulatory Technical Standards and official guidance on the implementation of PSD2	https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2
EMV	Integrated circuit card specification for payment systems **www.emvco.com**
Global Payments	For the purposes of this guide, all references to Global Payments refers to GPUK LLP trading as Global Payments
ISO 3166 (all parts)	Codes for representation of countries and their subdivisions
ISO 4217	Codes for representation of currencies and funds
PCI DSS	Payment Card Industry Data Security Standards; maintained by PCI SSC.
PCI SSC	Payment Card Industry Security Standards Council www.pcisecuritystandards.org

3. Glossary of Terms

3D Secure (3DS)	A form of strong customer authentication used by ecommerce merchants and card issuers to verify the cardholder's identity. It's sometimes known by the Card Scheme branding, for example, Visa Secure (previously Verified by Visa), Mastercard Identity Check and American Express SafeKey.
3DS2	Any version of 3DS versions 2.0 or above. Some documentation refers to it as EMV 3DS.
3DS Requestor Initiated Message (3RI)	A 3DS authentication message made by the merchant when the cardholder isn't present, used to refresh the CAV in some circumstances, like split shipment or delayed despatch.
Acquirer	The entity processing the card transaction (Global Payments). Note: in PSD2 official wording, the acquirer is called a PSP.
ACS	Access Control Server. The card issuer system (usually a third party), that provides the authentication services on a 3DS transaction.
Cardholder	The person that's paying for the goods or service.
Card Issuer	The organisation issuing the card product.
CAV	Cardholder Authentication Value. The generic name for the secure cryptogram generated by the 3DS process.
CAVV	Cardholder Authentication Verification Value. The Visa name for the CAV.
Customer Initiated Transaction	An ecommerce transaction performed by the cardholder. In the context of a Credential on File transaction (below) it's performed using their card details that were previously stored with the merchant.
Credential on File (CoF)/Stored Credentials	Where a cardholder gives express permission for a merchant to store their card details for future use by either the merchant or the cardholder. The first transaction (when the cardholder gives permission to store the details) should be subject to SCA to give the card issuer confidence that the subsequent transactions are legitimate. Subsequent transactions using the stored details can be initiated by the cardholder or the merchant. If the merchant initiated transaction will be for a set amount, it can be considered a Recurring Transaction. See the Global Payments document: Stored Credential-Technical Implementation Guide:
Gateway	PSD2 official documentation calls a PSPs a gateway.
Merchant Initiated Transaction (MIT)	A transaction carried out by the merchant (subject to prior cardholder agreement), with no action from the cardholder, using previously stored card details. For the purposes of SCA Exemption flagging, MITs aren't fixed amounts.
'One leg out' transaction	In the context of PSD2, a transaction where one of the parties (either the merchant, acquirer or card issuer) isn't located in the European Economic Area (EEA).
Payment Service Provider (PSP)	In this guide, PSP means a software and services provider to ecommerce merchants, which facilitates authentication and payments. Note: in PSD2 official wording, the PSP is called a Gateway
Point of Sale (POS) device	In the context of this guide, a physical terminal used by face to face merchants that enable their customers to pay by card.
Recurring Transaction	The new definition for one of a series of merchant initiated CoF transactions for a fixed amount. It the amount is variable then it is considered an MIT.
TAVV	The Visa name for the secure cryptogram generated by the 3DS process done with a stored payment token rather than a card number.
UCAF	Universal Cardholder Authentication Field. The Mastercard name for the CAV.

4. PSD2 and SCA

What's PSD2?
On the 14th September 2019, a new regulation is being introduced that'll change the way online payments take place within the European Economic Area (EEA). From this date, most ecommerce payments will have to undergo SCA to validate that the payer is who they say they are. For ecommerce payments made on card, a new authentication protocol is being introduced by the Card Schemes called 3D Secure 2 (3DS2) to comply with the regulation.

The Second Payment Services Directive (PSD2) is a fundamental piece of payments related legislation in Europe, which entered into force in January 2016. PSD2 is the product of a review of the original Payment Services Directive and requires Payment Service Providers (PSPs) to make a significant number of changes to existing operations. The Directive required that all Member States implement these rules as national law by 13th January 2018, with the exception of certain rules around SCA and secure communication, implementation of which will run to a different timetable.

PSD2 is a significant evolution of existing regulation for the payments industry. It aims to increase competition in an already competitive industry, bring into scope new types of payment services, enhance customer protection and security and extend the reach of the Directive.

The key changes introduced by PSD2 can be grouped into four main categories:
- market efficiency and integration;
- consumer protection;
- competition and choice;
- security.

Some more specific changes include:
- Extension of scope to all currencies and one-leg out payment transactions
- Changes to the scope of the exclusions
- Passporting, authorisation rules and supervision of payment institutions
- Consumer protection
- New providers and new payment services
- Operational and security risk management and incident reporting
- Requirements for strong customer authentication and secure communication

How does PSD2 effect cards processing?
PSD2 mandates that all electronic payments, whether face to face or remote, must be completed using SCA. This requirement enters into law in all EEA countries (including the UK) from 14th September 2019.

What's SCA?
Strong Customer Authentication - SCA - requires a cardholder to authenticate themselves for a transaction using at least two independent factors. These factors can be:
- Something the customer knows (for example a PIN number or password)
- Something the customer is (biometrics, such as a fingerprint or voice recognition)
- Something the customer is in possession of (for example a card or a mobile phone)

For ecommerce transactions, 3D Secure 1 (3DS1) meets the basic criteria to support SCA, but 3DS2 has more functionality allowing it to provide a better SCA experience.

How does this affect my business?
At the simplest level:
- A chip and PIN transaction in a store already adheres to SCA, but a Contactless transaction doesn't
- A fully authenticated 3DS transaction adheres to SCA, but an ecommerce transaction without 3DS doesn't.

Under PSD2, card issuers are obliged to challenge and potentially decline non SCA transactions to protect their cardholders. So all merchants will be affected in some way to a greater or lesser extent. This guide explains how and what you need to do to be ready for 14th September 2019.

After 14th September 2019, a card issuer has the choice to approve, decline or request SCA (if it wasn't done already) for a transaction.

Does SCA apply to all transactions?
No. Some transactions, where SCA isn't possible, are out of scope and some transactions can be exempt.

Out of Scope Transactions
The following transaction types are out of scope for SCA:

- Unattended parking and transport terminals - but all other unattended devices are currently required to support chip and PIN
- Mail Order and Telephone Order (MOTO) transactions, subsequent Recurring Transactions and Merchant Initiated Transactions (Stored Credential Transactions, also known as Credential on File Transactions)
- 'One leg out' transactions - it may not be possible for UK based merchants to apply SCA to transactions when the card issuer isn't located in the EEA. Merchants should still attempt SCA for all transactions and let the Card Schemes\ACS service providers handle the geography
- Anonymous transactions (for example those done with anonymous pre-paid cards) aren't subject to the SCA mandate. Card issuers won't be obliged to request SCA

But, in all these cases, the transactions must be flagged clearly and correctly (with a parking terminal Merchant Category Code (MCC), or as a Mail Order or a Credential on File Transaction, for example) or the card issuer may choose to challenge the merchant for SCA. If the cardholder can't be contacted or provide SCA, the transaction will not go ahead.

Exempt Transactions
Some transactions are exempt from SCA, but they must be correctly identified as such and the exemption exists within strict parameters. The card issuer has the right to challenge any exemption and request SCA, so exceptions don't remove the need to develop the capability to process transactions securely.

Contactless cards in a face to face environment are exempt up to certain issuer parameters. The card issuer is obliged to monitor spending, and when a threshold has been reached, the cardholder must perform a chip and PIN transaction to reset the counters. In the UK that means 'dipping' the card in the terminal and entering their PIN.

Ecommerce transactions have various potential exemptions that can be used (see Section 6.1). It's important to understand that if they're used, the merchant (who's requesting the SCA exemption) is liable for all fraud and chargebacks. It's for this reason that Global Payments won't be permitting all merchants to use these exemptions. Exemptions may only be used with the express consent of Global Payments (see Section 6.1).

Visa and Mastercard are still defining some of the rules and functionality around the use of exemptions at the time that Global Payments are producing version 1 of this guide. It's expected that functionality and services will expand in scope in future versions of this guide and the ASTS.

How does a card issuer challenge the SCA exemption?
In the event that a card issuer receives either an authorisation request for a non-secure transaction, or a request to use an exemption, they're required to validate if this is a low risk transaction. If they determine the transaction not to be low risk, they'll instruct that the transaction needs to be completed securely, and in this scenario, Global Payments will return a decline code of 65 to the merchant or the PSP.

Decline code 65 has been used previously but no longer means that the transaction has been declined by the card issuer. Rather, a return code of 65 now means that SCA is required before the transaction can be approved and that the authorisation request needs resubmitting (see Sections 5 and 6 for what this means in different implementations).

5. Requirements for POS Terminals

What's changing?
For Contactless cards, in the event the card issuer's frequency or value thresholds have been achieved, they'll require the cardholder to do a chip and PIN transaction by returning the 65 response code instead of approving the transaction. Your terminals should show this (as per the screen below), and allow the cardholder to complete a chip and PIN transaction.

For chip and PIN, and mobile phone payments, there are no additional requirements.

Doesn't that already happened today?
Today some card issuers have counters on the card chip that request 'step up' to chip and PIN. The request happens the moment the card is tapped and it doesn't happen very often.

From 14th September all card issuers are required to do this, and they'll do it from their issuing systems, so there may be a short delay before you get the message. The rules about when they're obliged to request SCA are quite stringent and it's likely to happen more often than before.

What do I need to do?
- Ensure that you and your staff understand what's happening and be ready to reassure cardholders there's no problem with their card or their account, just that it's an extra security check requested by their card issuer.
- If you rent your terminals from Global Payments, you don't need to do anything. The terminals will display the information on the screen as above.
- If you own your own terminal or rent it from another supplier, then you need to contact the provider and ensure that no software update is needed.
- No change is required to the authorisation or settlement messages that are sent to Global Payments, you just need to ensure that cardholders will be prompted to do a chip and PIN transaction when the terminal receives a specific code to do so (as explained below).

Global Payments will send a return code 65 with the prompt text (shown above). It's important that your terminal treats this return code separately from other non-zero return codes (which all mean decline). If your terminal doesn't display the accompanying text correctly, or treats all non-zero return codes the same, then it may cause customer dissatisfaction if they think their card is being declined because of a problem.

See Appendix B for the table of valid return codes that you may receive from Global Payments, what they mean and what should be displayed on the screen.

When are Contactless terminals out of scope for SCA?
The regulators acknowledge that in some circumstances it may not be possible for terminals to go online for SCA or have PIN pads to enter a PIN. For example, some parking meters or unattended vending machines. Those terminals don't need to support SCA. Card issuers should be able to identify such transactions using existing data points and not respond with code 65.

6. Requirements for Ecommerce Merchants

What's changing?
SCA will be required for all ecommerce transactions. Merchants that haven't adequately authenticated their customers, (or given an adequate reason as to why they haven't or can't) will run the substantial risk that card issuers will decline their transactions.

When a transaction is sent for authorisation, in addition to approving or declining, a card issuer can decline a transaction with the return code of "65 SCA REQUIRED".

If an ecommerce merchant receives an authorisation response with a return code of 65, they must make an attempt to SCA the transaction before submitting a new authorisation request.

What do I need to do?
- At a minimum, you need to support 3DS1
- Correctly flag transactions in your authorisation and clearing records, where the cardholder isn't available to be authenticated (see sections below).
- Adopt 3DS2 to take advantage of extra functionality available to improve the customer experience and possible SCA exemptions (see section below)

I don't support 3DS today, what do I need to do?
Contact your PSP urgently and ensure that you can submit 3DS authentication requests before 14th September 2019.

I support 3DS1 today, do I need to do anything?
You don't need to do anything before 14th September to meet the minimum requirements, but you may wish to contact your PSP to discuss upgrading to 3DS2. 3DS2 offers a wealth of improved functionality, including additional data fields, mobile optimisation and SCA exemptions.

When will I have to support 3DS2?
The Card Schemes haven't yet mandated 3DS2 nor issued a specific end date for 3DS1, but they have clearly stated that in the future they intend to issue a sunset date for 3DS1.

What are the advantages of supporting 3DS2?
3DS version 2.0 and above versions have been designed to deliver a smooth checkout experience across all devices so you don't have to worry about abandonment on mobile devices. 3DS2 authentication will be available across all integration types to enable you to implement the solution effectively and with ease. It allows merchants to pass much more data to the card issuer to give them greater confidence in the authentication and it also gives issuers and merchants more ways of authenticating cardholders (such as the support for biometric verification using a thumb print).

How do I implement 3D Secure?
Global Payments has developed the capability to process 3D2 transactions, but you need to first speak with your Gateway (PSP), to understand how this is implemented on your website.

Our Global Payments E-Commerce Platform (formerly known as Realex Payments) will be supporting 3DS2 when the regulation takes effect in 2019 and will be introducing solutions that make it easy to comply with the SCA requirements. Over the coming months, we'll be upgrading our authentication solution and if you're a user of our E-Commerce Platform, you'll be provided with further details of what you have to do to comply with the new regulation.

If you use a third party provider for your ecommerce services, you'll need to contact your supplier to obtain further information of the changes they're making. Our 3DS2 solution can be used alongside your existing gateway solution if required.

Do all transactions have to be subject to SCA?
No. Some transactions are out of scope (see below). A merchant may also request an exemption. If the merchants supports 3DS2 they may request that their transaction is exempt if the transaction (or the merchant) meets certain criteria. SCA Acquirer Exemption is explained in Section 6.1.

Out of Scope Transactions **–** Some Cardholder Not Present (CNP) transactions are out of scope for SCA. In order that issuers are aware and don't request SCA on those transactions, it's important that they're correctly flagged as per the Global Payments ASTS requirements. Also, because some of the Card Schemes request that they're also flagged as Acquirer Exemptions, additional exemption flags are required (see Section 6.1).

What amount should I authenticate?
You should authenticate the full amount that the goods or service will cost. If the cost will be split across 10 payments of £10 (for example) you should authenticate £100, not £10.

There's no specific ruling on variation of amounts, but guidance is that if the actual authorisation amount is greater than 15% of the authentication amount a second authentication should take place. This may require using the 3RI functionality of 3DS2 to request a second authentication cryptogram when the cardholder isn't present.

A cardholder has the right to contact their card issuer and initiate a dispute if they don't recognise the amount they actually pay because it was different from the authentication amount.

It's also possible to authenticate with a zero amount if the transaction amount isn't be known, for example, when storing cardholder credentials for future use.

How long's the authentication valid for?

The CAV (cryptogram) that secures the authentication response is valid for 30 days under Card Scheme Rules. This means that if there's a delay in shipping the goods and you need to authorise the transaction (for all or just some of the original amount) after 30 days, you should do a 3RI authentication exemption request to the card issuer's 3DS service again before submitting the authorisation request as a merchant initiated transaction. This will reduce the likelihood of the card issuer rejecting the authorisation.

If it's been a long time since the last authorisation of a MIT or Recurring Transaction, for example, an annual subscription, it's also recommended to seek an authentication exemption to get a new cryptogram.

6.1 Acquirer Exemptions from SCA

What are the Exemptions?
The Card Schemes have each created a list of possible exemptions, detailed below, that they expect to be flagged correctly if used. All current possible exemptions are listed here for completeness, but inclusion in the below list doesn't imply that Global Payments will support them all, or that Global Payments will permit all merchants to use them.

Remote payment low value exemption – this exemption can be used if the value of the transaction is less than €30. The card issuer is obliged to keep a counter and reject the exemption request if the cumulative spend since the last use of SCA by the card reaches €100 or a count of five transactions.

Transaction Risk Analysis (TRA) exemption – this exemption can be used if the acquirer or card issuer has a fraud rate below specific thresholds depending on transactions amounts.

Trusted beneficiary exemption – this is sometimes known as 'merchant whitelisting'. To use this exemption, a cardholder must give explicit agreement to their card issuer to exempt a specific merchant from performing SCA for all subsequent transactions. The mechanism for doing this will vary depending on the card issuer and the Card Scheme. Comprehensive mechanisms to support this exemption are unlikely to be ready by September 2019.

Secure corporate payment exemption – it's expected that this exemption is to apply to business to business payments. The PSD2 RTS Article 17 gives provision for it, but it's still unclear from the regulator whether or not commercial cards, 'lodged cards' (a commercial card given to a third party such as a travel agent to book travel on behalf of the company) or other business cards fall into this category. The use of this exemption is still being defined. It's expected that card issuers will manage this by defining explicit ranges within the ACS service.

Merchant Initiated Transaction - this exemption is for subsequent Credential on File transactions for different amounts. It should be used if the amount varies from the transaction amount at the time when the cardholder's details were stored (and SCA was performed), and the cardholder undertakes no action to execute a payment.

This exemption should be used in conjunction with the Credential on File flagging, and Scheme Reference Data to ensure that the issuer doesn't request SCA.

Recurring Transaction - this exemption is for subsequent Credential on File transactions for a fixed amount. If the amount of the original transaction (at the time when the cardholder's details were stored, and SCA was performed) and all future amounts will be the same, this exemption should be used in conjunction with the Credential on File flags to ensure that the issuer doesn't request SCA.

SCA delegation – in this scenario, the card issuer gives the merchant authority (and responsibility) to uniquely identify the cardholder on its behalf. Functionality for how this will be achieved is still being formulated by the Card Schemes.

When can I use the exemptions?
Some exemptions are Card Scheme specific but the Global Payments system is Card Scheme agnostic. Global Payments will handle any Card Scheme specific rules on behalf of merchants. If a merchant flags an exemption that isn't required by the relevant Card Scheme, then the Global Payments systems will manage the request. If an unsupported exemption is used in an invalid scenario, the Global Payments systems will return an error code of 65 requiring the merchant to seek SCA.

The use of exemptions by Global Payments customers falls into three categories:

1. Credential on File Transactions
- Merchant Initiated Transaction
- Recurring Transactions

Used for **subsequent** credential on file transactions as appropriate (see Section 6.3.2). The first transaction during which the cardholder gives permission for their card to be stored should always be fully authenticated.

2. Low Risk Transactions
- Low value exemption
- Transaction Risk Analysis exemption

However, merchants should only use these exemption after consultation with Global Payments. Low risk transaction exemptions require additional validation to be completed by the merchant to demonstrate the transaction is low risk.

3. Future allowances
- Trusted beneficiaries exemption
- Secure corporate payment exemption
- SCA delegation

Merchants shouldn't use these exemptions.

Global Payments doesn't currently support these three exemptions, since at the time of writing this guide, the Card Scheme use of them isn't fully defined. It's expected that support will be adopted at a future date and will require further changes to the technical specification.

How do I use an exemption?
Exemptions should be requested in two steps:
1. By making an exemption request to the 3DS service. The instructions on how to do this will be provided by your PSP and are outside of the scope of this guide.
2. If the card issuer's 3DS service grants the exemption, this should then be flagged in the authorisation (and settlement) message submitted to Global Payments. See Section 6.3.1 of this guide for the specific fields and values that need to be set.

Example message flows are listed in Appendix A

What are the implications of using the exemptions?
The primary implication is that by using one of the exemptions, the merchant is taking liability for the transaction and any subsequent fraud is counted towards Global Payments ability to offer exceptions to its customers. This liability is why Global Payments expects to be consulted and give permission for the use of all exemptions apart from those used for Credential on File transactions (for which the merchant is already liable today).

What are the implications of incorrectly or over using the exemptions?
Global Payments will be reviewing the use of exemptions by individual merchants.

In addition to taking on increased financial liability, incorrect or unauthorised use of exemption flagging may result in card issuers excessively declining your transactions, Card Scheme penalties or other financial sanctions.

6.2 3DS2 Technical Requirements

What additional fields are required for 3DS2?
As well as the fields required today for 3DS1, the following additional values must be set for all transactions authenticated or exempted using 3DS2 or above.

Authorisation:

Auxiliary Data Record Type 01: Ecommerce

(Only some specific fields are highlighted below in this guide. All applicable fields should be populated not just those listed below.)

Num	Name	F/V	Type	Len	M/O/C	Value
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'
31.3.7	Cardholder Authentication Value	V	AB	32	M	Up to 32 characters supplied by the merchant. **Mastercard:** UCAF is 32 characters long, **Visa:** CAVV\TAVV is 28 characters long. This field will be populated for all authorisations where 3DS was attempted, whether this resulted in the cardholder being authenticated or not.
31.3.8	Group Separator	F	GS	1	C_1	1D (HEX)
31.3.9	3D Secure Program Protocol	F	N	2	C	'01' = 3D Secure 1.x '02' = 3D Secure 2.x This field must be set to '02' to identify a 3DS2 transaction.
31.3.10	Group Separator	F	GS	1	C_1	1D (HEX)
31.3.11	Directory Server Transaction ID	F	A	36	C	The Directory Server ID used in the 3DS process. This field must be populated for a 3DS2 transaction.
31.3.12	Group Separator	F	GS	1	C_1	1D (HEX)

Settlement:

All fields in Sub-Record Format Type 41 should be populated when the authorisation request was authenticated by 3DS2.

Sub-Record Format Type 41: 3D Secure Sub-Record

This sub-record must be populated fully when Field 31.3.9 and Field 31.3.11 are populated in the authorisation request Auxiliary Data Record Type 01 Ecommerce (sub-type 01) and is mandatory for all 3DS2 transactions whether authenticated or not.

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	'01' = 3D Secure 1.x '02'= 3D Secure 2.x This values must be set to '02' for all 3DS2 transactions
3	Customer Instruction Modifier	+6	N	3	000 = Authenticated transaction 216 = SCA Exempted Transaction 217 = Transaction out of scope for SCA See Section 6.3.1 (Settlement) below for guidance on this field. The default value should be '000'.
4	Reserved For Future Use	+9	A	10	Space Filled
5	Transaction Code	+19	N	2	'41'
6	Card Holder Authentication Value	+21	A	48	The result of the 3DS secure transaction (UCAF or CAVV) as an alphanumeric string right justified and padded with spaces. This value should be populated for non-authenticated transactions when returned from the ACS. This value must be populated for all 3DS2 transactions
7	Reserved For Future Use	+69	N	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 3DS Server. Space filled if not applicable. This value must be populated for all 3DS2 transactions
126 Byte Record					

6.3 SCA Exemption Technical Requirements

6.3.1 Additional Fields for SCA Exemption

For merchants submitting SCA exempt transactions, there are specific fields that must be populated in both authorisation and settlement messages.

Authorisation:

There's one new field in Auxiliary Data Record Type 01 Ecommerce to indicate that an SCA exemption is being requested.

Auxiliary Data Record Type 01: Ecommerce

Num	Name	F/V	Type	Len	M/O/C	Value
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'
31.3.19	SCA Exemption Indicator	F	AB	4	O	Code indicating which (if any) SCA exemption has been granted or is being requested. See Table 14 SCA Exemption Indicator

ASTS Table 14 – SCA Exemption Indicator

The SCA Exemption Indication Indicator is a PSD2 requirement used to indicate why SCA wasn't applied to an ecommerce transaction. The indicator may be used either to indicate the exemption was already granted by the card issuer's 3DS server (in which case the transaction will have an accompanying CAV cryptogram) or to directly request an exemption from the card issuer (in which case there'll be no accompanying CAV). Merchants using these flags will take liability and lose chargeback rights for all of the transaction.

The card issuer reserves the right to decline any authorisation request with or without an SCA Exemption Indicator, or cryptogram.

An explanation of the different exemptions is provided above in Section 6.2.

	Feature	8	4	2	1
First Position:	Low value exemption				X
	Trusted risk analysis exemption			X	
	Trusted merchant exemption		X		
	Secure corporate payment exemption	X			
Second Position:	Merchant Initiated Transaction				X
	Recurring Transaction			X	
	SCA delegation		X		
	Reserved	X			
Third Position:	Reserved				X
	Reserved			X	
	Reserved		X		
	Reserved	X			
Fourth Position:	Reserved				X

	Feature	8	4	2	1
	Reserved			X	
	Reserved		X		
	Reserved	X			

The field takes the form of a bitmap because originally the Card Schemes indicated that more than one exemption could be used for a transaction. Standard 70 was therefore written to support multiple values. Subsequently, the Card Scheme Rules have changed and now only one exemption may be requested at any one time.

Merchants should only submit one SCA Exemption Indicator per authorisation request.

If a merchant tries to submit a transaction with multiple exemption flags, Global Payments will discard values and only send one based on the following rules:

- MIT or Recurring Transactions take highest priority
- The second position takes precedent over the first
- The lowest value in a position takes precedent

If a merchant submits an authorisation request for an exemption type that Global Payments doesn't support, Global Payments may decline the transaction with a return code of 65.

The SCA Exemption Indicator in the authorisation request should match that submitted in the authentication request to the ACS server.

Settlement:

Field number 3 in Sub-Record Format Type 41 SD Secure Sub-record should be set with one of three different values depending on whether the transaction was subject to SCA, exempt or a subsequent Credential on File Transaction. For full details of the use of this sub-record see Section 6.2 (Settlement) above.

Num	Name	POS	Type	Len	Value
…					
3	Customer Instruction Modifier	+6	N	3	000 = Authenticated transaction 216 = SCA exempted transaction 217 = Transaction out of scope for SCA This value should be set to '217' if the authorisation request was exempted as a Recurring Transaction or Merchant Initiated Transaction and '216' for all other SCA exempted transactions. If the transaction was subject to SCA then the value will be '000'.
…					
126 Byte Record					

6.3.2 Recurring Transaction and Credential on File Transactions

The instructions in this guide are in addition to the existing requirements for Credential on File Transactions whether the future transaction is to be a Recurring Transaction for a fixed amount or a Merchant Initiated Transaction. See the Global Payments Stored Credentials Technical Implementation Guide for full details, which can be found on our website at www.globalpaymentsinc.co.uk. It's within our Customer Centre, under the Stored Credential Transactions tile.

The initial transaction of any Credential on File should always be subject to SCA.

For subsequent transactions when the cardholder isn't present:

- Recurring Transactions (when the amount is a fixed amount every time) should be exempted by setting a value of 0200 in field 31.3.19
- Merchant Initiated Transactions (when the amount is variable) should be exempted by setting a value of 0100 in field 31.2.19

For subsequent transactions when the cardholder is present (a CIT), SCA should be performed using the cardholders stored credentials.

Best Practice

If a merchant supports 3DS2, to ensure a better acceptance rate from card issuers, merchants are encouraged to send a 3RI Recurring Transaction or Merchant Initiated Transaction SCA exemption request to the card issuers ACS server for authentication exemption. The resulting 3DS2 values and appropriate SCA Exemption Indicator should then be set in the authorisation message as per this guide.

The cryptogram is only valid for 30 days and so if the period between authorisation requests is greater than this period, the authentication process should be repeated.

Appendix A – Example Message Flows

3DS1 Authenticated Transaction

A 3DS1 authentication message flow is the same structure as the 3DS2 flow (below), however, the transaction carries less information in the authentication request. This makes it more likely that the card issuer will challenge the cardholder to identify themselves.

3DS2 Authenticated Transaction

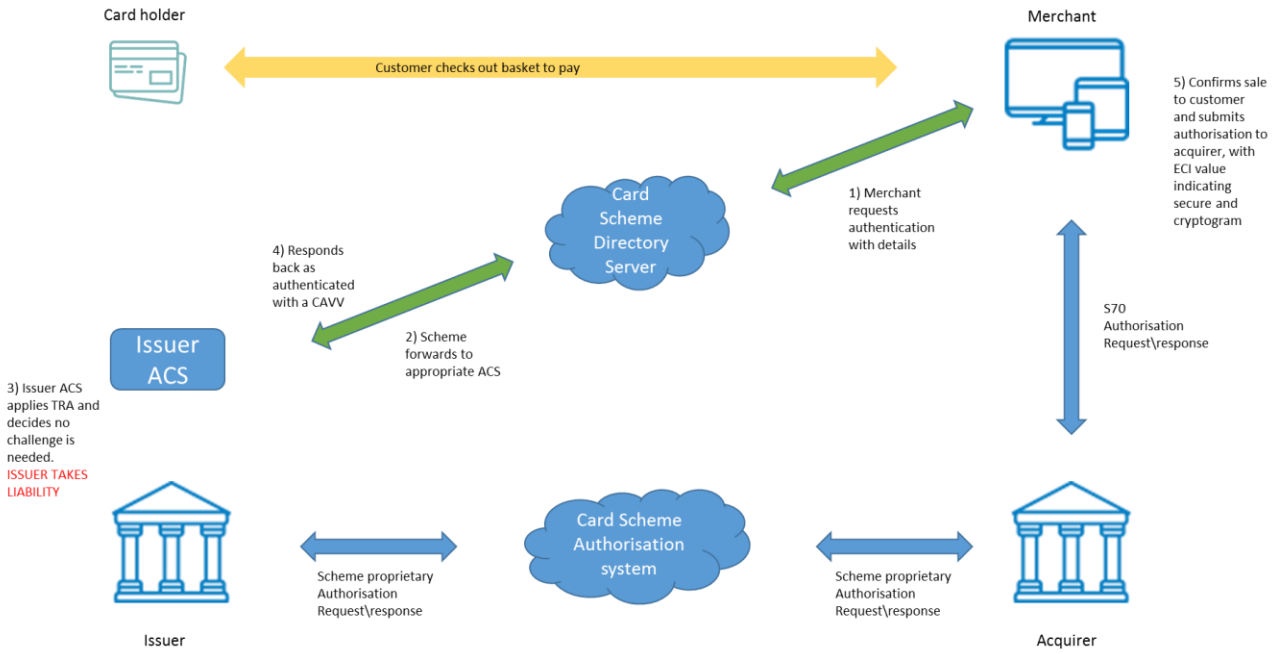
A 3DS2 transaction carries substantially more cardholder information in the authentication request. This makes it more likely that the card issuer won't feel the need to challenge the cardholder to identify themselves but be able to perform risk analysis and decide on the probability that the cardholder is genuine (see Fig 1 below).

1. Cardholder checks out basket to pay for goods.
2. Merchant/PSP sends 3DS authentication request to the card issuer's ACS server.
3. Card issuer's ACS server chooses either to:
   a. perform risk analysis (and not challenge the cardholder), or
   b. challenge the cardholder to authenticate themselves.
4. Card issuer's ACS responds back with:
   a. cardholder authenticated, or
   b. cardholder not authenticated.
5. Merchant/PSP sends an authorisation request to the acquirer with appropriate values from the ACS (see Section 6.2 – 3DS2 Technical Requirements).
6. Acquirer formats the authorisation request to the Card Scheme specification and sends to the card issuer via the Card Scheme.
7. Card issuer either approves or declines the transaction*.

*Even though the cardholder was authenticated, the transaction may still be declined for various reasons, for example, the cardholder doesn't have the funds to pay.

Fig 1

Standard 3DS v2 flow: Issuer Transaction Risk Analysis applied



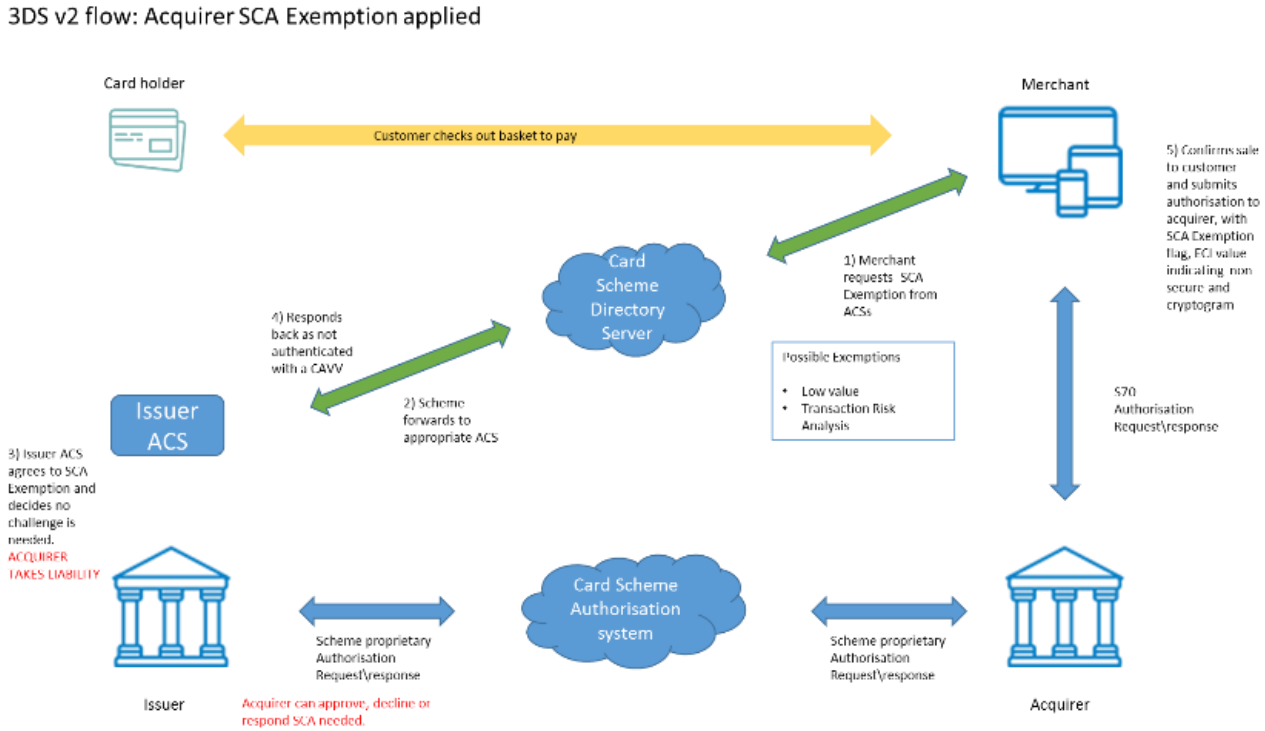
3DS2 Authenticated SCA Exempted Transaction

In order for an exemption request to be made, the merchant\PSP must support the 3DS2 authentication request. The ACS server uses the additional data available to it to access the request. For low value exemptions, the ACS server will be required to keep a running total of exempted transaction values and if the threshold for that card has been reached, it'll issue the cardholder challenge (see Fig 2 below).

1. Cardholder checks out basket to pay for goods.
2. Merchant/PSP sends 3DS authentication request to the card issuer's ACS server with an SCA exemption reason.
3. Card issuer's ACS server choses either to:
   a. accept the exemption request (and the merchant then takes liability), or
   b. decline the exemption request and challenge the cardholder to authenticate themselves (if authenticated the card issuer has liability).
4. Card issuer's ACS responds back with appropriate response and accompanying details including a secure cryptogram.
5. Merchant/PSP sends either: (see section 6.3.1)
   a. an authorisation request to the acquirer with appropriate values from the ACS and the SCA Exemption Indicator that matches the request to the ACS, or
   b. an authorisation request to the acquirer with appropriate values from the ACS.
6. Acquirer formats the authorisation request to the Card Scheme specification and sends to the card issuer via the Card Scheme.
7. Card Issuer either approves, requests SCA, or declines the transaction*.

*Even though the cardholder was authenticated, the transaction may still be declined for various reasons, for example, the cardholder doesn't have the funds to pay.

Fig 2



Out of Scope SCA Exempted Transaction

As stated in Section 6.3.2, best practice is to treat Recurring Transactions and Merchant Initiated Transactions as acquirer exemptions, but this isn't compulsory. Merchants (especially those who only support 3DS1 and have no option to seek an exemption from the ACS) may submit these transactions directly to the acquirer (see below).

1. Merchant/PSP instigates an authorisation request to the acquirer using cardholder details that were previously stored following a fully authenticated transaction. The transaction should be submitted as per Credential on File rules and supported by the SCA Exemption Indicator appropriate for that transaction type (see Section 6.3.2).
2. Acquirer formats the authorisation request to the Card Scheme specification and sends to the card issuer via the Card Scheme.
3. Card issuer either approves, requests SCA, or declines the transaction*.

*If the card issuer is unsure that the transaction is merchant initiated, it may request SCA. Declined transactions shouldn't be submitted to settlement.

Appendix B – Authorisation Response Codes

Authorisation Response Codes and Message Text

The following table details the response codes that may be returned to a terminal along with the message text that will be returned for the terminal to display and/or print.

Response Code	Message Text	Reason
00	AUTH CODE: NNNNNN	Approve
00	ACCOUNT VALID	Approval For Account Verification Transactions
00	REVERSAL ACCPTD	Reversal Accepted
02	CALL AUTH CENTRE	Referral
03	INVALID MERCHANT	Merchant Unknown / Merchant Number has not been set up on authorisation system
04	DECLINE & PICKUP	Issuer Requires Card To Be Retained
05	DECLINE	Decline (N/A reversals)
05	CANNOT AUTHORISE	Terminal ID is unrecognised
05	CONSENT REVOKED	Cardholder Has Ended A Recurring Transaction / Instalment
05	INVALID TRAN	Transaction Not Allowed At Terminal
05	CARD EXPIRED	Expired Card
05	NOT AUTHORISED	Allowable Number Of PIN Tries Exceeded
05	ACCOUNT INVALID	Decline For Account Verification Transactions
10	AUTH CODE: NNNNNN	Partial/Alternative Amount Approval
13	INVALID AMOUNT	Invalid Amount
14	INVALID CARD NO	Invalid Account Number
21	TERM DEACTIVATED	Invalid Terminal ID
30	BAD FORMAT	Format Error In Authorisation Request
30	BAD AMOUNT	Format Error In Authorisation Request
30	BAD EXPIRY DATE	Format Error In Authorisation Request
30	INVALID TRACK 2	Format Error In Authorisation Request
30	BAD ACCOUNT	Format Error In Authorisation Request
30	BAD DESCR	Format Error In Authorisation Request
55	PIN Error	Incorrect PIN
65	Chip Read Req., Insert Card	Strong Customer Authentication required

Appendix C – Abbreviations

The tables below explain abbreviations used in the ASTS extracts in this guide.

Field Types

Abbreviation	Meaning
A	**Alphanumeric:** Alphanumeric fields are to be left justified and padded with spaces unless specifically defined as otherwise in this specification.
N	**Numeric:** Numeric fields are to be right justified and padded with leading zeros unless specifically defined as otherwise in this specification.
AB	**8 bit binary data converted into printable hexadecimal.** **Note:** All alpha characters must be upper case.

Table Headings

Abbreviation	Meaning
POS	Position
Type	The type of data to be submitted in the field (see 3.1 for full details)
Len	Field Length
F/V	Fixed or Variable
M/O/C	Mandatory, Optional or Conditional

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