Monetico Paiement

Migration guide for integration of the 3DSecure V2 protocol

Remote payment page and integrated payment page (iFrame)

EURO INFORMATION

CONTENTS

1 Introduction

The technical standards that complete PSD2 introduce new rules in terms of the security of online transactions. These provisions will impact transactions made on your retail website. They come into effect on 14 September 2019.

What's changing:

PSD2 imposes two-factor authentication procedures (also called "strong authentication").

To make a purchase on your retail website, your buyers will have to authenticate themselves using at least two of the following elements:

- Knowledge: something that only the buyer knows (e.g. a password, a code, etc.);
- Possession: something that only the buyer possesses (e.g. mobile phone, chip card, etc.);
- Inherence: something that the buyer is (e.g. finger print, voice or facial recognition, etc.).

To meet the requirements of this directive, Monetico Paiement is integrating the new version of 3D Secure. The purpose of this is to:

- reinforce security of your payments;
- add further security to your payment collections;
- help you to meet regulatory requirements;
- ensure a smooth process for your buyers by enhancing transaction data (provision of additional data, such as delivery address, cart content, etc.) in order to allow your buyer's bank to concretely determine whether a strong authentication is necessary or not.

This document references the specific changes brought about by the integration of the 3D Secure 2.0 protocol. You can read the full documentation for the remote payment page and the integrated payment page here

2 Service URLs

A migration to the URLs of Monetico Paiement is required. These URLs are listed in sections 2.1 and 2.2.

The historical URLs will no longer be in use:

- https://paiement.creditmutuel.fr
- https://ssl.paiement.cic-banques.fr
- https://ssl.paiement.banque-obc.fr

2.1 The test environment, known as "sandbox"

The role of our test environment is to allow you to validate your developments. Of course, all transactions made by our test payment environment are fictive and do not lead to a real bank transaction.

To make payment requests in this environment, we provide you with test bank cards. They can be accessed by clicking the "Test Card" icon on the payment page.

The test environments are available at the following addresses:

- Payment form:
  https://p.monetico-services.com/test/paiement.cgi

- Capturing and re-crediting services:
  https://payment-api.e-i.com/test/capture_paiement.cgi
  https://payment-api.e-i.com/test/recredit_paiement.cgi

The test merchant dashboard allows you to manage and control payments made in the test environment. It is available at the following address:

- https://www.monetico-services.com/fr/test/

2.2 In Production

After validating your developments and requesting the production launch of your POS from centrecom@e-i.com, you can contact the production server, available here:

- Payment form:
  https://p.monetico-services.com/paiement.cgi

- Capturing and re-crediting services:
  https://payment-api.e-i.com/capture_paiement.cgi
  https://payment-api.e-i.com/recredit_paiement.cgi

You can view payments made on your POS via the merchant dashboard at the following address:

- https://www.monetico-services.com/fr/

We draw your attention to the fact that requests sent to the production server will be actual transactions.

3 Updating the payment interface

3.1 "Request" interface

The "Request" interface which initiates a payment request will be modified and will take the following elements into account:

- A review of the options field
- The addition of two new call settings and strict verification of input settings
- Use of the new MAC algorithm
- Deletion of the parameter url_retour

3.1.1 Review of the options field

Currently, the "Options" field, integrated into the MAC algorithm, is defined as follows:

options	List of options used (may be empty). Each option is separated from the others by the “&” character. If the option has a value, the name is separated from the value by "=".	**Example:** opttest=abc&optbis=123

This is a field that aggregates the values of several separate settings. The values of this field are now divided into the dedicated settings.

The options concerned are:

- aliascb
- forcesaisiecb
- 3dsdebrayable
- libelleMonetique
- desactivemoyenpaiement

As well as all fields dedicated to Cofidis payment means.

3.1.2 Example

An incoming request with the 3dsdebrayable and aliascb setting will be modified as follows:

Request before: …&options=aliascb=MonClient1&3dsdebrayable=1…
Request after: …&aliascb=MonClient1&3dsdebrayable=1&…

3.1.3 Addition of two new call settings

Two new settings have been added. They are described below.

It is important to note that as of now, the mandatory fields must all be provided at the time of the call and must comply with the technical restrictions listed in the technical documentation.
As for optional fields, they:

1. May not be provided
2. May be provided empty
3. If provided with a value, they must comply with the restrictions listed in the technical documentation.

Field	**contexte_commande**
Presence	Mandatory
Description	Information concerning the order: detail of cart, shipping and invoicing addresses and technical context. The technical description is available below
Format **Possible value(s)**	Data in JSON - UTF-8 format encoded in base64.

Field	**ThreeDSecureChallenge**
Presence	Optional
Description	Merchant's preference concerning the 3D Secure v2.X challenge
Format **Possible value(s)**	"no_preference": choice by default "challenge_preferred" "challenge_mandated": challenge required "no_challenge_requested" "no_challenge_requested_strong_authentication": no challenge requested – the customer's strong authentication has already been performed by the merchant. "no_challenge_requested_trusted_third_party": no challenge requested – request for exemption because the merchant is a trusted third party. "no_challenge_requested_risk_analysis": no challenge requested – request for exemption for a reason other than one already mentioned (for example: small amount)
Example	challenge_preferred

3.1.4 Deletion of the parameter url_retour

The url_retour parameter of the payment page is no longer used, so it is removed from the list of parameters accepted by our service. It is therefore appropriate to no longer send it.

3.1.5 Use of the new MAC algorithm

To calculate the **MAC**, refer to the documentation in appendix.

This new calculation must be implemented to be able to use 3DSecure 2.0 and to fill in the new fields. The merchant kits have been updated in this regard and are available here: Monetico kits.

3.2 «Response» interface

The «Response» interface that notifies your server of the result of processing a payment will be modified and will include the following elements:

- Provision of additional fields and modification of structure
- Use of the new MAC algorithm

3.2.1 Provision of additional fields and modification of structure

There is a new authentication field.

Field	authentification
Description	Document JSON/UTF-8 encoded in base 64 containing the information related to the customer's authentication, notably for 3D Secure.
Addition	**Link** to the document structure.

In the case of 3D Secure 1.0, this field will replace the fields currently provided, which are VERes, PARes and status3DS. They are repeated in the JSON structure of this new field. The examples here present this change.

3.2.2 Use of the new MAC algorithm

To calculate the **MAC**, refer to the documentation in appendix.

4 Update of the collection / cancellation of payment request interface

The purpose of the "capture_paiement" service is to allow merchants to collect or to cancel a payment request.

The "texte-libre" setting has been deleted from this service.

5 Update of the refund interface

The purpose of the "recredit_paiement" service is to allow merchants to refund their customers some or the full amount of their purchase, securely.

The "texte-libre" setting has been deleted from this service.

6 Appendices

6.1 MAC algorithm

The seal (to put in the MAC field) is calculated using a cryptographic hash function combined with a secret key in line with RFC 2104 specifications.
This function will generate a seal based on data to be certified and the merchant's security key in its operational form.

The data to be certified is structured:

- in the form of a sequence *Field_name=Field_value*,
- with the elements separated by the "*" character,
- listed in alphabetical order

When calling a Monetico Paiement service, the seal must take into account all the parameters sent - valued or not - recognized by the platform, and only these.

When checking the seal on the "Response" interface, all parameters are taken into account.

Note:
The order used is based on the ASCII code. In addition, it is case sensitive:

- first, the numbers from 0 to 9,
- then, characters in UPPER CASE,
- lastly, characters in lower case.

For special characters, refer to the ASCII table

6.2 Detail of the JSON document "contexte_commande"

6.2.1 General points and exclusions

This field contains the information concerning the context of the order and is used during the "Request" phase.

This information is necessary to implement 3D Secure (2.X) and to fight fraud.

Note that the MOTO operation is excluded from 3D Secure, therefore this information is not mandatory in this new mode of operation.

Up to four objects are present in the root of the document.

The presence column can be read as follows:

- Mandatory: this field / node must be provided
- Optional: this field does not have to be provided
- Mandatory if applicable: if the value exists in the context of the order, it must be provided. Example: stateOrProvince exists in the United States

JSON field	Description	Presence	Detail
billing	Billing address	Mandatory	link
shipping	Shipping address	Mandatory if applicable	link
shoppingCart	Customer's cart	Optional	link
client	Customer information	Optional	link

6.2.2 Detail of the "billing" object

JSON field	Presence	JSON type	Detail
civility	Optional	String	link
name	Optional	String	link
firstName	Optional	String	link
lastName	Optional	String	link
middleName	Optional	String	link
address	Optional	String	link
addressLine1	Mandatory	String	link
addressLine2	Optional	String	link
addressLine3	Optional	String	link
city	Mandatory	String	link
postalCode	Mandatory	String	link
country	Mandatory	String	link
stateOrProvince	Mandatory if applicable	String	link
countrySubdivision	Optional	String	link
email	Optional	String	link
phone	Optional	String	link
mobilePhone	Optional	String	link
homePhone	Optional	String	link
workPhone	Optional	String	link

6.2.3 Detail of the "shipping" object

JSON field	Presence	JSON type	Description
civility	Optional	String	link
name	Optional	String	link
firstName	Optional	String	link
lastName	Optional	String	link
address	Optional	String	link
addressLine1	Mandatory if applicable	String	link
addressLine2	Optional	String	link
addressLine3	Optional	String	link
city	Mandatory if applicable	String	link
postalCode	Mandatory if applicable	String	link
country	Mandatory if applicable	String	link
stateOrProvince	Mandatory if applicable	String	link
countrySubdivision	Optional	String	link
email	Optional	String	link
phone	Optional	String	link
shipIndicator	Optional	String	link
deliveryTimeframe	Optional	String	link
firstUseDate	Optional	String	link
matchBillingAddress	Optional	Boolean	link

6.2.4 Detail of the "shoppingCart" object

JSON field	Presence	JSON type	Description
giftCardAmount	Optional	Number	link
giftCardCount	Optional	Number	link
giftCardCurrency	Optional	String	link
preOrderDate	Optional	String	link
preorderIndicator	Optional	Boolean	link
reorderIndicator	Optional	Boolean	link
shoppingCartItems	Optional	Table of items	link

6.2.4.1 Detail of the "shoppingCartitems" object

JSON field	Presence	JSON type	Description
name	Optional	String	link
description	Optional	String	link
productCode	Optional	String	link
imageURL	Optional	String	link
unitPrice	Mandatory	Number	link
quantity	Mandatory if applicable	Number	link
productSKU	Optional	String	link
productRisk	Optional	String	link

6.2.5 Detail of the "client" object

JSON field	Presence	JSON type	Description
civility	Optional	String	link
name	Optional	String	link
firstName	Optional	String	link
lastName	Optional	String	link
middleName	Optional	String	link
address	Optional	String	link
addressLine1	Optional	String	link
addressLine2	Optional	String	link
addressLine3	Optional	String	link
city	Optional	String	link
postalCode	Optional	String	link
country	Optional	String	link
stateOrProvince	Optional	String	link
countrySubdivision	Optional	String	link
email	Optional	String	link
birthLastName	Optional	String	link
birthCity	Optional	String	link
birthPostalCode	Optional	String	link
birthCountry	Optional	String	link
birthStateOrProvince	Optional	String	link
birthCountrySubdivision	Optional	String	link
birthdate	Optional	String	link
phone	Optional	String	link
nationalIDNumber	Optional	String	link
suspiciousAccountActivity	Optional	Boolean	link
authenticationMethod	Optional	String	link
authenticationTimestamp	Optional	String	link
priorAuthenticationMethod	Optional	String	link
priorAuthenticationTimestamp	Optional	String	link
paymentMeanAge	Optional	String	link
lastYearTransactions	Optional	String	link
last24HoursTransactions	Optional	String	link
addCardNbLast24Hours	Optional	String	link
last6MonthsPurchase	Optional	String	link
lastPasswordChange	Optional	String	link
accountAge	Optional	String	link
lastAccountModification	Optional	String	link

6.2.6 Description of attributes

Attribute	**accountAge**
Description	Date of creation of customer account on the merchant's site.
Format	String
Restrictions	Type YYYY-MM-DD where YYYY = year in 4 digits, MM = month in 2 digits, DD = day in 2 digits (ISO 8601)

Attribute	**addCardNbLast24Hours**
Format	Integer
Description	Number of attempts to add the customer card on the retail website during the past 24 hours.

Attribute	**address**
Description	Customer's full address (number, street, additional information)
Format	String
Restrictions	Up to 255 characters

Attribute	**addressLine1**
Description	Contains the number and street name
Format	String
Restrictions	Up to 50 characters

Attribute	**addressLine2**
Description	Contains the number and street name
Format	String
Restrictions	Up to 50 characters

Attribute	**addressLine3**
Description	Any additional information concerning the address that is not entered in lines 1 and 2 of the address.
Format	String
Restrictions	Up to 50 characters

Attribute	**authenticationMethod**
Description	Method of authenticating the customer on the retail website.
Format	String
Possible values	"guest": no authentication "own_credentials": use of an account open on the retail website "federated_id": federated identity "issuer_credentials": identifiers supplied by the issuer "third_party_authentication" "fido": use of FIDO authentication

Attribute	**authenticationTimestamp**
Description	Date and UTC time of the customer's authentication on the retail website.
Format	String
Restrictions	Type YYYY-MM-DD**T**HH-mm-SS**Z** where YYYY = year in 4 figures, MM = month in 2 figures, DD = day in 2 figures, HH = time in 2 figures, mm = minutes in 2 figures, SS = seconds in two figures (ISO 8601)

Attribute	**birthCity**
Description	City of birth
Format	String
Restrictions	Up to 50 characters

Attribute	**birthCountry**
Description	Country of birth
Format	String
Restrictions	Country code in 2 characters as per ISO 3166-1 alpha-2

Attribute	**birthCountrySubdivision**
Description	Geographic code of the entity of the country of birth
Format	String
Restrictions	Follow ISO 3166-2.
Help	https://en.wikipedia.org/wiki/ISO_3166-2 https://en.wikipedia.org/wiki/ISO_3166-2:FR

Attribute	**birthdate**
Description	Birth date as per ISO 8601 format
Format	String
Restrictions	Type YYYY-MM-DD where YYYY = year in 4 figures, MM = month in 2 figures, DD = day in 2 figures

Attribute	**birthLastName**
Description	Birth name
Format	String
Restrictions	Up to 45 characters

Attribute	**birthPostalCode**
Description	Postal code of birthplace
Format	String
Restriction	Up to 10 characters

Attribute	**birthStateOrProvince**
Format	String
Restrictions	ISO 3166-2
Description	Geographic code of the state or province of birth (if applicable).
Help	https://fr.wikipedia.org/wiki/ISO_3166-2:US https://fr.wikipedia.org/wiki/ISO_3166-2:CA

Attribute	**city**
Format	String
Restrictions	Up to 50 characters
Description	City May contain the CEDEX.

Attribute	**civility**
Description	Civility
Format	String
Restrictions	Up to 32 alphabetical characters. No punctuation. Examples: "Mr, "Mrs"

Attribute	**country**
Description	Country code
Format	String
Restrictions	ISO 3166-1 alpha-2

Attribute	**countrySubdivision**
Description	Geographic code of the entity of the country
Format	String
Restrictions	ISO 3166-2
Help	https://en.wikipedia.org/wiki/ISO_3166-2 https://en.wikipedia.org/wiki/ISO_3166-2:FR

Attribute	deliveryTimeframe
Description	Indicates the delivery time-frame for the order.
Format	String
Possible values	"same_day" "overnight" "two_day" "three_day" "long": more than three days "other" "none": no shipment

Attribute	description
Description	Description of an item.
Format	String
Restrictions	Up to 2048 characters.

Attribute	email
Format	String
Restrictions	Up to 100 characters.
Description	Email

Attribute	firstName
Description	First name
Format	String
Restrictions	Up to 45 characters

Attribute	firstUseDate
Description	Date on which the shipping address was first used.
Format	String
Restrictions	ISO 8601 format Type YYYY-MM-DD where YYYY = year in 4 figures, MM = month in 2 figures, DD = day in 2 figures

Attribute	giftCardAmount
Description	Amount used to buy gift cards / codes, expressed in the smallest unit of currency.
Format	Integer
Restrictions	Maximum of 12 meaningful numbers

Attribute	giftCardCount
Description	Number of gift cards purchased
Format	Integer
Restrictions	Maximum of 2 meaningful numbers

Attribute	giftCardCurrency
Format	String
Restrictions	3 alphabetical characters (e.g.: EUR). ISO 4217
Description	Currency of the gift card purchased

Attribute	homePhone
Description	Telephone number
Format	String
Restrictions	Up to 18 numerical characters with "+" as the first character, followed by the country code, a hyphen "-" and then the number
Example	The French mobile number 05 12 34 56 78 will be written "+33-512345678"
Help	https://en.wikipedia.org/wiki/List_of_country_calling_codes https://en.wikipedia.org/wiki/E.123 https://en.wikipedia.org/wiki/E.164

Attribute	imageURL
Description	URL pointing to an image associated with an item.
Format	String
Restrictions	Up to 2000 characters.

Attribute	last24HoursTransactions
Format	Integer
Description	Number of transactions (completed or aborted) made by the customer with any payment method registered on the retail website in the past 24 hours.

Attribute	last6MonthsPurchase
Description	Number of purchases with this payment method in the past 6 months.
Format	Integer

Attribute	lastAccountModification
Description	Date of last modification of the customer account (including new billing address, new delivery address, new payment method registered).
Format	Type YYYY-MM-DD where YYYY = year in 4 figures, MM = month in 2 figures, DD = day in 2 figures ISO 8601

Attribute	lastName
Description	Family name.
Format	String
Restrictions	Up to 45 characters.

Attribute	lastPasswordChange
Description	Date on which the customer changed their password or reset their account for the last time.
Format	Type YYYY-MM-DD where YYYY = year in 4 figures, MM = month in 2 figures, DD = day in 2 figures ISO 8601

Attribute	lastYearTransactions
Format	Positive whole number or zero
Description	Number of transactions (completed or aborted) made by the customer with any payment method registered on the retail website in the past year.

Attribute	matchBillingAddress
Description	Indicates whether the shipping or billing addresses are the same.
Format	Boolean

Attribute	middleName
Description	Middle name(s)
Format	String
Restrictions	Up to 150 characters

Attribute	mobilePhone
Description	Mobile telephone number
Format	String
Restrictions	Up to 18 numerical characters with "+" as the first character, followed by the country code, a hyphen "-" and then the number The French mobile number 06 12 34 56 78 will be written "+33-612345678"
Help	https://en.wikipedia.org/wiki/List_of_country_calling_codes https://en.wikipedia.org/wiki/E.123 https://en.wikipedia.org/wiki/E.164

Attribute	name
Description	Last Name and First Name
Format	String
Restrictions	Up to 45 characters

Attribute	nationalIDNumber
Description	Number of ID document
Format	String
Restrictions	Up to 255 characters

Attribute	paymentMeanAge
Description	Date on which the card was added to the customer account (on the retail website).
Format	YYYY-MM-DD where YYYY = year in 4 figures, MM = month in 2 figures, DD = day in 2 figures ISO 8601

Attribute	phone
Description	Telephone number
Format	String
Restrictions	Up to 18 numerical characters with "+" as the first character, followed by the country code and then the number The French mobile number 06 12 34 56 78 will be written "+33612345678"
Help	https://en.wikipedia.org/wiki/List_of_country_calling_codes https://en.wikipedia.org/wiki/E.123 https://en.wikipedia.org/wiki/E.164

Attribute	postalCode
Description	Post or zip code
Format	String
Restrictions	Up to 10 characters

Attribute	preOrderDate
Description	For a pre-order, date on which the goods will be available.
Format	Type YYYY-MM-DD where YYYY = year in 4 figures, MM = month in 2 figures, DD = day in 2 figures ISO 8601

Attribute	preorderIndicator
Description	Indicates whether it is a pre-order.
Format	Boolean

Attribute	priorAuthenticationMethod
Description	Customer's previous authentication method on the retail website.
Format	String
Possible values	"guest": no authentication "own_credentials": use of an account open on the retail website "federated_id": federated identity "issuer_credentials": identifiers supplied by the issuer "third_party_authentication" "fido": use of FIDO authentication

Attribute	priorAuthenticationTimestamp
Description	Date and UTC time of the customer's previous authentication on the retail website.
Format	String
Restrictions	Type YYYY-MM-DDTHH-mm-SSZ where YYYY = year in 4 figures, MM = month in 2 figures, DD = day in 2 figures, HH = time in 2 figures, mm = minutes in 2 figures, SS = seconds in two figures ISO 8601

Attribute	productCode
Description	Indicates the type of product.
Format	String
Possible values	"adult_content" "coupon" "default": default value (if no other code is suitable) "electronic_good": (not including software) "electronic_software" "gift_certificate" "handling_only": admin fees "service": service delivered to the customer "shipping_and_handling" "shipping_only" "subscription": to a website or other

Attribute	productRisk
Description	Indicates the level of risk related to a product.
Format	String
Possible values	"low" "normal" "high"

Attribute	productSKU
Description	Reference that the merchant gives to an item.
Format	String
Restrictions	Up to 255 characters

Attribute	quantity
Format	Integer
Description	Expresses a quantity (e.g. a number of items)

Attribute	reorderIndicator
Description	"True" if, and only if, the customer has already made an identical order.
Format	Boolean

Attribute	shipIndicator
Format	String
Description	Chosen shipping method.
Possible values	"digital_goods": (no shipping). "travel_and_event": (no shipping). "billing_address": delivery to the billing address. "verified_address": Shipping to an address that has already been used. "another_address": Shipping to a new address. "pick-up": Shipping to a collection point. "other".

Attribute	shoppingCartItems
Description	Table containing the items in the cart.
Format	Table of items (type "shoppingCartItem")

Attribute	stateOrProvince
Description	Geographic code of the state or province (if applicable).
Format	String
Restrictions	ISO 3166-2
Help	https://en.wikipedia.org/wiki/ISO_3166-2:US https://en.wikipedia.org/wiki/ISO_3166-2:CA

Attribute	suspiciousAccountActivity
Description	Indicates whether the suspicious activities on the customer account have been reported by the merchant.
Format	Boolean

Attribute	unitPrice
Description	Amount expressed in the smallest unit of currency (for example, in centimes for the EURO)
Format	Integer
Restrictions	Maximum of 12 meaningful numbers

Attribute	**workPhone**
Description	Work telephone number
Format	String
Restrictions	Up to 18 numerical characters with "+" as the first character, followed by the country code, a hyphen "-" and then the number The French mobile number 05 12 34 56 78 will be written "+33-512345678"
Help	https://en.wikipedia.org/wiki/List_of_country_calling_codes https://en.wikipedia.org/wiki/E.123 https://en.wikipedia.org/wiki/E.164

6.3 Detail of the JSON document "authentication"

This field contains the information concerning the card holder's authentication and is provided during the «Response» phase.

JSON field	Description	Details
status	Result of authentication	link
protocol	Protocol used	link
version	Version of protocol	link
details	Details specific to the protocol and to the version	link

General information (status, protocol, version) is situated at the root of the JSON document. It is possible to base business processing on this information only, mainly by using the "status" field. The "details" field can provide a more in-depth analysis of the operation of the 3D Secure process.

6.3.1 Detail of the "details" object

JSON field	Description	Details
liabilityShift	Transfer of liability	link
VERes	Result contained in the VERes message	link
PARes	Result contained in the PARes message	link
ARes	Result contained in the ARes message	link
CRes	Result contained in the CRes message	link
merchantPreference	Merchant's preference	link
transactionID	ID of the transaction	link
authenticationValue	Cryptogram linked to the transaction	link
status3DS	3D Secure 1.X exchange indicator	link
disablingReason	Reason for disabling 3D Secure 1.X	link

6.3.2 Description of attributes

Attribute	**status**
Description	Indicates the result of the authentication
Format	String
Possible values	• "authenticated": The authentication was successful. • "authentication_not_performed": The authentication could not be completed (technical or other problem). • "not_authenticated": The authentication failed. • "authentication_rejected": The authentication was rejected by the issuer. • "authentication_attempted": An authentication attempt took place. Authentication could not be completed but a proof was generated (CAVV) • "not_enrolled": The card is not enrolled for 3DS • "disabled": In the event of using the 3D Secure disabling option only usable within the framework of 3D Secure 1.X

Attribute	**protocol**

Description	Protocol used for authentication
Format	String
Possible values	3DSecure

Attribute	**version**
Description	Version of protocol
Format	String
Possible values	1.0.2 2.1.0

Attribute	**liabilityShift**
Description	Indicates whether there is a transfer of liability to the issuing bank
Format	String
Possible values	"Y": The issuing bank is responsible for the risk. "N": The merchant is responsible for the risk. "NA": Impossible to determine, or not applicable.
Presence	For 3D Secure 2.X only.

Attribute	**VERes**
Description	Verification of enrolment of a card for 3D Secure 1.X.
Format	String
Possible values	"Y": card enrolled for 3D Secure 1.X. "N": card not enrolled for 3D Secure 1.X. "U": Technical problem when verifying the card's eligibility
Presence	For 3D Secure 1.X only.

Attribute	**PARes**
Description	Result of 3D Secure authentication
Format	String
Possible values	"Y": Authentication successful. "U": Technical problem during authentication. "N": Authentication failed. "A": No authentication, but the card holder's bank is taking responsibility for the risk.
Presence	For 3D Secure 1.X only.

Attribute	ARes
Description	The ARes message is the ACS response from the issuer to the AReq message. It may indicate that the card holder has been authenticated or that an additional interaction between the card holder is necessary to complete the authentication. There is just one ARES message per transaction.
Format	String
Possible values	"Y": Authentication successful without challenge. "R": Authentication rejected by the issuer "C": Challenge requested. "U": The ACS did not respond correctly. "A": Authentication could not be completed but a proof was generated "N": Authentication failed without challenge.
Presence	For 3D Secure 2.X only.

Attribute	CRes
Description	The CRes message is the ACS response to the CReq message. It may indicate the card holder's result of authentication or, for a model based on an application, also indicate that additional interaction from the card holder is necessary to complete authentication.
Format	String
Possible values	"Y": Authentication successful after challenge. "N": Authentication failed after challenge.
Presence	For 3D Secure 2.X only.

Attribute	merchantPreference
Description	Indicates the merchant's preference concerning the 3D Secure 2.X authentication process. This is only a preference and it may not be approved by the issuing banks.
Format	String
Possible values	"no_preference": No preference expressed. "challenge_preferred": preference for challenge. "challenge_mandated": challenge forced. "no_challenge_requested": No challenge requested. "no_challenge_requested_strong_authentication": no challenge requested – the customer's strong authentication has already been performed by the merchant. "no_challenge_requested_trusted_third_party": no challenge requested – request for exemption because the merchant is a trusted third party. "no_challenge_requested_risk_analysis": no challenge requested – request for exemption for a reason other than one already mentioned (for example: small amount)

Attribute	**transactionID**
Description	Unique ID related to the transaction.
Format	String / UUID (RFC 4122)
Possible values	UUID (RFC 4122)
Presence	For 3D Secure 2.X only.

Attribute	**authenticationValue**
Description	Binary date encoded in base64 in 28 characters
Format	String
Presence	For 3D Secure 2.X only.

Attribute	**status3DS**
Description	3D Secure 1.X exchange indicator
Format	Integer
Possible values:	-1: the transaction did not take place according to the 3D Secure protocol and the risk of non-payment is high 1: the transaction took place according to the 3DS protocol and the risk of non-payment is low 4: the transaction took place according to the 3DS protocol and the risk of non-payment is high
Presence	For 3D Secure 1.X only.

Attribute	**disablingReason**
Description	For 3D Secure 1.X only, coupled with the 3D Secure disable option. Indicates the disabling reason.
Format	String
Possible values	commercant: explicitly disabled by the merchant by sending the appropriate value in the form of the "Out" phase seuilnonatteint (threshold not reached): disabled because the amount of the transaction does not equal the amount configured by the merchant scoring: disabled for scoring reason

6.3.3 Example

Below is an example of the JSON authentication document within the framework of 3D Secure 2.0.

```
{
   "status":"authenticated",
   "protocol":"3DSecure",
   "version":"2.1.0",
   "details":{
      "liabilityShift":"Y",
      "ARes":"C",
      "CRes":"Y",
      "merchantPreference":"no_preference",
      "transactionID":"555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a",
      "authenticationValue":"cmJvd0I4SHk3UTRkYkFSQ3FYY3U="
   }
}
```

After base64 encoding:

```
ewoJInN0YXR1cyIgOiAiYXV0aGVudGljYXRlZCIsCgkicHJvdG9jb2wiIDogIjNEU2VjdXJlIiwKCSJ2ZXJzaW9uIiA
iMi4xLjAiLAoJImRldGFpbHMiIDogCgl7CgkJImxpYWJpbGl0eVNoaWZ0IiA6ICJZIiwKCQkiQVJlcyIgOiAiQyIsCg
kJIkNSZXMiIDogIlkiLAoJCSJtZXJjaGFudFByZWZlcmVuY2UiIDogIm5vX3ByZWZlcmVuY2UiLAoJCSJ0cmFuc
2FjdGlvbklEIiA6ICI1NTViZDlkOS0xY2YxLTRiYTgtYjM3Yy0xYTk2YmM4YjYwM2EiLAoJCSJhdXRoZW50aWN
hdGlvblZhbHVlIiA6ICJjbUp2ZDBJNFNIazNVVFJrWWtGU1EzRllZM1U9IgoJfQp9
```

6.4 Management of the 3D Secure authentication protocol

Authentication of bank card holders during an act of payment takes place via the 3D Secure protocol. This ensures that the person entering the bank card information on the payment page is legitimate for this purchase: they are asked to perform an additional action (enter a code, authentication via a mobile application, etc.) to authenticate them as the bank card holder.

Until now, this authentication phase was based on version 1 of the secure communication protocol between the different 3D Secure actors.

In 2019, version 2.1 of this protocol will be applied. This new version will be the subject of a gradual upgrade throughout the second half of the year and probably into 2020. This means that, during this period, a transaction could take place with the 3D Secure V1 or the 3D Secure V2 protocol. The version of the protocol used will be defined depending on the holder's bank card: the issuing bank will decided which authentication version to use. These decisions depend partly on the BIN but not only.

In order to handle this transition period in the best possible way, you will find below some explanations regarding the impacts this will have on the Monetico Paiement platform.

It is important to note that as the networks (VISA, Mastercard, CB) are still finalising the specification of the standard, some information will change.

6.4.1 The payment request – "request" interface

During the payment request, two settings are available to indicate the behaviour of the Monetico Paiement solution with regard to 3D Secure authentication:

- 3dsdebrayable: this field is specific to the 3D Secure V1 protocol.
- ThreeDSecureChallenge: this field is specific to the 3D Secure V2 protocol.

Both fields can be provided during the payment request in order to ensure implementation of the required authentication behaviour, regardless of the version of protocol used for a payment.

The table below recommends which values to use depending on the preferred authentication scenario:

Preferred scenario	3dsdebrayable	ThreeDSecureChallenge
No preference	by choice	no_preference
Preferred authentication	0 or nothing	challenge_preferred
Authentication systematically requested	0 or nothing	challenge_mandated
No authentication requested	1	no_challenge_requested
No authentication requested, exemption type: strong authentication	1	no_challenge_requested_strong_authentication
No authentication requested, exemption type: trusted third party	1	no_challenge_requested_trusted_third_party
No authentication requested, exemption type: prior risk analysis carried out	1	no_challenge_requested_risk_analysis

Point of attention concerning the disabling option: if your POS is configured to automatically bypass the 3D secure authentication depending on the amount, any transaction for an amount less than the configured amount will be disabled within the framework of the 3D Secure V1 protocol: this equates to entering the value "3dsdebrayable" = 1 during a payment request.

6.4.2 Server-to-server notification of the payment result – "response" interface

The table below indicates the different scenarios encountered and the values returned by the Monetico Paiement platform.

For each status, you will find the different scenarios that may lead to this status and examples of the value of the "authentication" field

Scenario	Status	Results
The 3D Secure protocol was completed The card holder was authenticated by the issuing bank via its ACS authentication page.	**authenticated (link)**	**link**
The 3D Secure protocol was completed The card holder was authenticated by the issuing bank via its ACS authentication page (frictionless). Transfer of liability differs depending on the preference expressed by the merchant: see the table on liability shift for details.	**authenticated (link)**	**link**
The 3D Secure protocol was completed. The card holder was authenticated by the issuing bank without formal authentication (no input of an authentication code for example)	**authentication_attempted (link)**	**link**
The 3D Secure protocol was started. The card holder's bank considered that this payment is risky and rejected authentication.	**not_authenticated (link)**	**link**
The 3DSecure protocol was started. Authentication of the card holder via the holding bank's ACS authentication page was requested, but it was not completed (several wrong entries of the authentication code, cancellation of authentication by the holder, etc.)	**not_authenticated (link)**	**link**
The 3D Secure protocol was started. Following a technical problem, it could not be completed.	**authentication_not_performed (link)**	**link**
The 3D Secure protocol was triggered but a technical problem occurred preventing the card holder being authenticated by the issuer.	**authentication_not_performed (link)**	**link**
The 3D Secure protocol was started. The card holder's bank rejected the authentication.	**authentication_rejected (link)**	**link**
The card is not enrolled for the 3D Secure protocol.	**not_enrolled (link)**	**link**

Status	**authenticated (link)**
Scenario	The 3D Secure protocol was completed The holder was authenticated by the issuing bank via its ACS authentication page.

3DS v1 feedback interface	{
	"status":"authenticated",
	"protocol":"3DSecure",
	"version":"1.0.2",
	"details":{
	"VERes":"Y",
	"PARes":"Y",
	"status3ds":1
	}
	}

3DS v2 Feedback interface	{
	"status":"authenticated",
	"protocol":"3DSecure",
	"version":"2.1.0",
	"details":{
	"liabilityShift":"<See specific table>",
	"ARes":"C",
	"CRes":"Y",
	"merchantPreference":"<preference expressed in Out phase>",
	"transactionID":"555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a",
	"authenticationValue":"cmJvd0I4SHk3UTRkYkFSQ3FYY3U="
	}
	}

Status	**authenticated (link)**
Scenario	The 3D Secure protocol was completed The card holder was authenticated by the issuing bank via its ACS authentication page (frictionless). Transfer of liability differs depending on the preference expressed by the merchant: see the table on liability shift for details.
3DS v1 Feedback interface	Not applicable

3DS v2 Feedback interface	{
	"status":"authenticated",
	"protocol":"3DSecure",
	"version":"2.1.0",
	"details":{
	"liabilityShift":"<See specific table>",
	"ARes":"Y",
	"merchantPreference":"<preference expressed in Out phase>",
	"transactionID":"555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a",

	"authenticationValue":"cmJvd0I4SHk3UTRkYkFSQ3FYY3U=" } }
Status	**authentication_attempted (link)**
Scenario	The 3D Secure protocol was completed. The card holder was authenticated by the issuing bank without formal authentication (no input of an authentication code for example)

3DS v1 Feedback interface	{
	"status":"authentication_attempted",
	"protocol":"3DSecure",
	"version":"1.0.2",
	"details":{
	"VERes":"Y",
	"PARes":"A",
	"status3ds":4
	}
	}

3DS v2 Feedback interface	{
	"status":"authenticated",
	"protocol":"3DSecure",
	"version":"2.1.0",
	"details":{
	"liabilityShift":"<See specific table>",
	"ARes":"C",
	"CRes":"Y",
	"merchantPreference":"<preference expressed in Out phase>",
	"transactionID":"555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a",
	"authenticationValue":"cmJvd0I4SHk3UTRkYkFSQ3FYY3U="
	}
	}

Status	**not_authenticated (link)**
Scenario	The 3D Secure protocol was started. The card holder's bank considered this payment to be risky and rejected authentication.
3DS v1 Feedback interface	Not applicable

3DS v2 Feedback interface	{
	"status":"not_authenticated",
	"protocol":"3DSecure",
	"version":"2.1.0",
	"details":{
	"liabilityShift":"<See specific table>",
	"ARes":"N",
	"merchantPreference":"<preference expressed in Out phase>",
	"transactionID":"555bd9d9-1cf1-4ba8-b37c-

```
1a96bc8b603a"
   }
}
```

Status	**not_authenticated (link)**
Scenario	The 3D Secure protocol was started. Authentication of the card holder via the holding bank's ACS authentication page was requested, but it was not completed (several wrong entries of the authentication code, cancellation of authentication by the card holder, etc.)

3DS v1 Feedback interface	{
	"status":"not_authenticated",
	"protocol":"3DSecure",
	"version":"1.0.2",
	"details":{
	"VERes":"Y",
	"PARes":"N",
	"status3ds":4
	}
	}

3DS v2 Feedback interface	{
	"status":"not_authenticated",
	"protocol":"3DSecure",
	"version":"2.1.0",
	"details":{
	"liabilityShift":"<See specific table",
	"ARes":"C",
	"CRes":"N",
	"merchantPreference":"<preference expressed in Out phase>",
	"transactionID":"555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a"
	}
	}

Status	**authentication_not_performed (link)**
Scenario	The 3D Secure protocol was started. Following a technical problem, it could not be completed.

3DS v1 Feedback interface	{
	"status":"authentication_not_performed",
	"protocol":"3DSecure",
	"version":"1.0.2",
	"details":{
	"VERes":"U",
	"status3ds":4
	}
	}

3DS v2 Feedback interface	{
	"status":"authentication_not_performed",
	"protocol":"3DSecure",
	"version":"2.1.0",
	"details":{
	"liabilityShift":"<See specific table>",
	"ARes":"U",
	"merchantPreference":"<preference expressed in Out phase>",
	"transactionID":"555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a"
	}
	}

Status	**authentication_not_performed (link)**
Scenario	The 3D Secure protocol was triggered but a technical problem occurred preventing the holder being authenticated by the issuer.

3DS v1 Feedback interface	{
	"status":"authentication_not_performed",
	"protocol":"3DSecure",
	"version":"1.0.2",
	"details":{
	"VERes":"Y",
	"PARes":"U",
	"status3ds":4
	}
	}

3DS v2 Feedback interface	{
	"status":"authentication_not_performed",
	"protocol":"3DSecure",
	"version":"2.1.0",
	"details":{
	"liabilityShift":"<See specific table>",
	"ARes":"C",
	"CRes":"U",
	"merchantPreference":"<preference expressed in Out phase>",
	"transactionID":"555bd9d9-1cf1-4ba8-b37c-

	1a96bc8b603a" } }

Status	**authentication_rejected (link)**
Scenario	The 3D Secure protocol was started. The card holder's bank rejected the authentication.
3DS v1 Feedback interface	Not applicable

3DS v2 Feedback interface	{
	"status":"authentication_rejected",
	"protocol":"3DSecure",
	"version":"2.1.0",
	"details":{
	"liabilityShift":"<See specific table",
	"ARes":"R",
	"merchantPreference":"<preference expressed in Out phase>",
	"transactionID":"555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a"
	}
	}

Status	**not_enrolled (link)**
Scenario	The card is not enrolled for the 3D Secure protocol.

3DS v1 Feedback interface	{
	"status":"not_enrolled",
	"protocol":"3DSecure",
	"version":"1.0.2"
	}

3DS v2 Feedback interface	{
	"status":"not_enrolled",
	"protocol":"3DSecure",
	"version":"2.1.0"
	}

To complete the tables above, below are the liability shift values depending on the different scenarios and statuses returned by Monetico Paiement.

6.4.2.1 Frictionless scenarios

Authentication of the card holder via the ACS of the issuing bank was completed.	Status	Liability Shift
Yes - Authentication via the ACS of the card holder's bank necessary	**authenticated**	Issuer
	not_authenticated	Transaction rejected
No - No authentication via the ACS of the holder's bank necessary	**authenticated** (frictionless)	Merchant
	authentication_attempted (ARes = A)	Dependent on the network and type of card
	authentication_not_performed (ARes = U)	Dependent on the network and type of card
	authentication_rejected (ARes = R)	Transaction rejected
	not_enrolled	Merchant

6.4.2.2 Challenge scenarios

Authentication of the card holder via the ACS of the issuing bank was completed.	Status	Liability Shift
Yes - Authentication via the ACS of the card holder's bank necessary	**authenticated**	Issuer
	not_authenticated	Transaction rejected
No - No authentication via the ACS of the card holder's bank necessary	**authenticated** (frictionless)	Issuer
	authentication_attempted (ARes = A)	Dependent on the network and type of card
	authentication_not_performed (ARes = U)	Dependent on the network and type of card
	authentication_rejected (ARes = R)	Transaction rejected
	not_enrolled	Merchant