

3DS Back office details

Details on 3-D Secure transactions

For payments which are authenticated with 3-D Secure you may see details like this:

[blocked URL](#)

The values shown above depend on 3-D Secure version used for authentication and the card scheme.

Here are some details:

ECI value

The ECI value stands for "Electronic Commerce Indicator" and detailed overview can be found here: [ECI Codes](#)

3-D Version (Directory Server)

The Directory Server is managed by the card scheme (Mastercard, VISA, American Express, ...) where each card issuer is registered and can be identified by the BIN (Bank Identification Number).

The Directory Server "talks" to the Access Control Server which finally refers to the card issuer system.

For 3-D Secure processing all parties (scheme, issuer and PSP Acepta) have to agree on the same 3-D Secure version.

3-D Version (Processing)

This is the 3-D Secure version which has been agreed by all parties finally for 3-D Secure authentication.

It may happen that a specific issuer is not supporting 3-D Secure (Version 2.1.0, 2.2.0) by now and then automatically a fallback to Version 1.0 will happen.

Authentication Type

Current supported values for "authentication type" are:

Value	Meaning	Description
00	Frictionless	Issuer did not challenge for a strong cardholder authentication.
01	Static	Static password is used for cardholder authentication. Also used for 3DS1 non frictionless
02	Dynamic	Dynamic password (e.g. token or app) is used for a strong cardholder authentication.
03	OOB	OOB stands for "Out Of Band": Users verify transactions in their issuer's authentication service which can be issuers' website or app.
04	Decoupled	Will be supported with 3-D Secure 2.2, intended to support card holder authentication for merchant initiated transactions (MIT).

Challenge Indicator (Requested)

Value	Meaning	Description
01	No preference	No specific challenge indicator requested, default value.
02	No challenge requested	Merchant prefers that "no challenge" should be performed
03	Challenge requested: 3DS Requestor Preference	Merchant prefers that a "challenge" should be performed
04	Challenge requested:Mandate	There are local or regional mandates that mean that a challenge must be performed
05	No challenge requested	Transactional risk analysis is already performed
06	No challenge requested	Data share only
07	No challenge requested	Strong consumer authentication is already performed
08	No challenge requested	Utilise whitelist exemption if no challenge required
09	Challenge requested	Whitelist prompt requested if challenge required

Transaction Status

Value	Meaning	Description
-------	---------	-------------

Y	Authentication Verification Successful	Authentication has been completed successfully, i.e. ready for authorisation. It still may happen that the authorisation fails, e.g. due to low account balance.
N	Not Authenticated /Account Not Verified	Transaction denied
U	Authentication/ Account Verification Could Not Be Performed	Technical or other problem, as indicated in ARes or RReq
A	Attempts Processing Performed	Not Authenticated/Verified, but a proof of attempted authentication/verification is provided.
C	Challenge Required	Additional authentication is required using the CReq/CRes.
D	Challenge Required	Decoupled Authentication confirmed.
R	Authentication/ Account Verification Rejected	Issuer is rejecting authentication/verification and request that authorisation not be attempted.
I	Informational Only	3DS Requestor (merchant) challenge preference acknowledged.

Whitelist Status

Value	Meaning
Y	3DS Requestor (merchant) is whitelisted by cardholder
N	3DS Requestor (merchant) is not whitelisted by cardholder
E	Not eligible as determined by issuer
P	Pending confirmation by cardholder
R	Cardholder rejected
U	Whitelist status unknown, unavailable, or does not apply