verifone

3-D Secure 1

First of all, 3D means 3-domain (not 3-Dimensional): Issuer domain, Acquirer domain and interoperability domain (the schemes). The protocol was initially invented by Visa, and later on, adapted by other schemes. As usual, everyone names it differently, although the flows are exactly the same. Visa's 3DS product is called Verified by Visa, Mastercard is called SecureCode (which is now changed to Identity Check with enhanced functionalities), American Express has SafeKey, Discover/Diners calls the product ProtectBuy, etc. etc. No matter how different the names are, all the existing products have the same concept and process flow, which will be described in this blog. The only differences are the exact data exchanged, and the algorithms used to guarantee the authenticity and integrity of the 3DS operation. This will also explain in this blog.

Why 3-D Secure

The purpose of 3-D Secure is to safeguard the online payment by applying an additional authentication step of the cardholder before sending an authorization request to the card issuer. Before 3DS was introduced, the only authentication of an online payment is on the CVC2.

With the evolution of card-present payments, especially with the introduction of EMV, frauds in the payment industry has been shifted to the more vulnerable channel: online card-not-present payments. As you can imagine, hacking or brutal-force-attaching a CVV2 is not the most difficult thing. Therefore, schemes had to make the effort to secure the online channel as well. This is the key drive of the introduction of 3-D Secure 1.0.

What are the benefits for everyone

- For **Schemes**, offering 3DS product to the members reduces the disputes handling efforts of both the members and the scheme, increases the acceptance through better merchant confidences.
- For **Acquirers and Merchants**, 3DS helps to reduce the chargeback rates, hence provides better protection to merchants. At the same time, it would also increase the sales due to the improved confidence of the cardholders
- For **Issuers**, 3DS adds value to existing product offerings and provides confidences to cardholders when shopping online
- For **Cardholders**, 3DS improves the confidence when shopping online

How does 3-D Secure work

Before we dive into the flows, a few roles and terminologies need to be explained.

As mentioned earlier, 3D means the three domains that are involved in securing the online payments: issuer domain, acquirer domain and interoperability domain.

- **Issuer Domain**: responsible for managing the enrolment of their cards for 3DS service and authenticating the cardholders during the 3DS authentication.
- **Acquirer Domain**: responsible for onboarding the merchants and requesting for 3DS authentication during online payments. By requesting 3DS operation, the liability of the acquirer is shifted to the issuer for online CNP transactions
- **Interoperability Domain**: responsible for facilitating the exchange of requests/responses between the Issuer and Acquirer domains

Each domain, therefore, would need a technical component to facilitate the 3DS flow:

- **MPI (Merchant Plug-in)**: the acquirer domain component, which creates and processes payment authentication messages. This functionality may be performed by the acquirer or a third party
- **DS (Directory Server)**: the interoperability domain component, which is responsible to facilitate the message exchanges between MPI and ACS, as well as determining whether card/acquirer/merchant is participating in the 3DS services
- **ACS (Access Control Server)**: the issuer domain component, which mainly performs two tasks: 1. Verify if the given card number is enrolled for 3DS service; 2. Authenticate the cardholder for a specific transaction. This service can be either hosted by the issuer or third-party providers

A typical process flow of a card payment transaction with 3DS authentication is shown below.

In a very simple language, a complete 3DS operation consists of two steps:

1. Merchant “ASK” the issuer: "hey, can this card do 3DS?” If the issuer’s answer is NO, the flow ends.
2. If the answer to question 1 is YES. Then merchant redirects the cardholder to issuer’s authentication site to complete the authentication. And guess what, that’s it.

In short, 3DS is a separate flow, which happens before an authorization request is sent. The flow is taken care of by a web-based system that consists of MPI, DS and ACS. The communications between these systems are completely decoupled from the traditional card payment processing rail. WHY? Because: 1. It is difficult to embed such flow into the card payment rail, which is built on top of ISO 8583 that do not have such a concept; 2. It is easy for acquirers, issuers, schemes to implement the support without interrupting the normal card payments processing; 3. It is based on more advanced technology, which is easier to integrate (compare to the ISO), and do not require special hardware.

The detailed processing flow is explained as below:

- **Step 0**: Cardholder requested to pay for a purchase online
- **Step 1**: Merchant decides to use 3DS to authenticate the cardholder before sending an authorization. So merchant sends a Verification request (VEReq) to the MPI, which then routes the request to scheme DS. At a minimum, the following data are included in a VEReq: card PAN, expiry dates, transaction amount, currency, transactions date.
- **Step 2**: Scheme DS, when receiving the VEReq from MPI, checks if the combination of the merchant, acquirer and card number that is making the request has been enabled at scheme side. If not, such request will be directly rejected. Otherwise, DS will route the VEReq to ACS.
- **Step 3**: When receiving the VEReq, the issuer ACS will check the internal registration record to determine if the card has been enrolled for 3DS service.
- Step 4: Issuer responds to the VEReq with a VERes message. Depending on if the card has been enrolled at the issuer, the following responses can happen in the VERes:
- Status = Y (card enrolled), hence a redirect URL is included for cardholder authentication later
- Status = N (card not enrolled), hence a redirect URL is not included
- Status = U (unable to verify). This can happen when the issuer’s ACS server is down. In this case, a redirect URL is not included

WHY this step? Because merchant needs to first query the issuer to see if the card can be used for 3DS authentication.

- **Step 5 - 6**: Issuer’s response, VERes, is returned to the merchant. Hence, the merchant can make a decision based on the enrolment status of the card and its own risk policy. e.g. continue with the authentication (in case of Y), continue with authorization without 3DS (in case of N and U), or decline (in case of N and U)
- **Step 7**: In case the enrolment status of the card is Y, and a redirect URL is returned in the VERes message, MPI sends a Payment authentication request (PAReq) message to the ACS via the cardholder's browser. At the same time, the cardholder is redirected to the issuer’s redirect URL for authentication.
    - At a minimum, the following data need to be sent in the PAReq: merchant ID, merchant name, merchant country, merchant URL, transaction date & time, transaction amount, currency, card PAN, order description, a unique transaction identifier determined by the merchant/MPI (also called XID).
- **Step 8**: Cardholder interacts with the issuer’s authentication server to authenticate himself. The exact mechanism and authentication method is proprietary to the issuer. e.g. via a static password that was configured at the moment of the enrolment to the service, or a dynamic authentication method that is shared with issuer’s online banking, etc. Once the cardholder successfully authenticated himself, the issuer’s ACS responds with a Payment Authentication Response (PARes) message, indicating the results of the cardholder authentication.
    - PARes is a base64 encoded form of a few data. At a minimum, the following data are included in a PARes: 1. Data from the PAReq message: Merchant ID, merchant name, transaction date & time, transaction amount, currency, card PAN, card expiry, XID; 2. Data from the ACS: authentication result codes, hash of the order description, ECI (Electronic Commerce Indicator) and

most importantly a “cryptogram” of the authentication action (in Visa terminology, it is called CAVV, Cardholder Authentication Validation Value. In Mastercard terminology, it is called AAV, Accountholder Authentication Value).
    - **Note**: CAVV/AAV is a cryptogram generated using card PAN, expiry date, a unique number per transaction, and the authentication result code. WHY these values? At a minimum, CAVV/AAV should serve the purpose to guarantee the integrity of the card used for the payments, the result of the 3DS authentication, and also to make sure that a replay attack is not possible (hence the unique number, e.g. XID).
    - Depending on the outcome of the 3DS authentication, the following authentication result codes may be returned:
        - **Y**: Authentication is successful
        - **N**: Authentication fails
        - **A**: Authentication attempted (see the next sections for detail)
        - **U**: Unable to authenticate. e.g. Issuer’s ACS is down
- The ECI value will be set corresponding to the 3DS authentication result.

Note: PARes will always be returned irrespective of the authentication result, so does the CAVV/AAV.

- **Step 9**: Merchant receives back PARes. Based on the result of the authentication (Y, N, A or U), merchant makes decision on whether to decline the transaction (e.g. in case the result is N), proceed the transaction with 3DS (e.g. in case result is Y or A) or proceed the transaction without 3DS (e.g. in case result is U). This is completely depends on the risk policy of each individual merchant.
- **Step 10 - 12**: Suppose that merchant decided to proceed with authorization with 3DS (either fully authenticated or attempted), an authorization message is sent with the PARes data (most of the time, only ECI, CAVV and XID) to the acquirer, which routes the transaction to issuer via the relevant scheme.
- **Step 13: Issuer**, when receiving an authorisation request that includes 3DS data, validate the data with its ACS server. E.g. validate if the CAVV/AVV is valid, and if yes, validate if the requested transaction amount, currency, etc. matches with the data when 3DS was requested.
- **Step 14 - 16**: Issuer respond to the acquirer (hence the merchant) the decision on the transaction authorization (either approve or decline), including the result of the 3DS data validation (note: a failed 3DS validation does not necessarily lead to a decline of authorization, but does lead to an indication that the transaction has been DOWNGRADED to non-3DS)

What is an Attempted authentication and when do we get it?

Now you might ask: when do we get an attempted authentication? Good question! That brings us to another important topic: Stand-in or attempted service. The attempted service will be hosted either by the card issuer or the scheme. At the moment, the scheme hosted solution is most commonly used.

To encourage the merchant to do 3DS even if a card is not enrolled for the service or if issuer ACS is temporarily unavailable, a stand-in mechanism is introduced. Again, in a most simplified language: this is a service to provide a “proof” that merchant did make the effort to try 3DS, even though the card was not enrolled or the issuer ACS was unable to reach. However, the fact that the merchant made the try will be “incentified” by shifting their liability.

As I mentioned, there will be two scenarios when the Attempted service will be called.

Scenario 1: card is not enrolled for 3DS. If this is the case, and the card issuer has enabled attempted service, the VEReq message (to check if the card is enrolled) will get a YES response from the attempted service and a redirect url from the attempted service (rather than the ACS). When merchant tries to redirect the cardholder to this url, it immediately get redirected back to the merchant again, with a PARes which stated the authentication status as A (attempted).

Scenario 2: card is enrolled for 3DS, however, the issuer’s ACS is unavailable. Hence the attempted (or stand-in) service is triggered, which again returns a YES response to the VEReq, together with a redirect URL. When merchant tries to redirect the cardholder to this URL, it immediately gets redirected back to the merchant again, with a PARes which stated the authentication status as A (attempted).

Note: at the moment, more and more issuers are subscribed to scheme's stand-in service. Hence, you would notice that more than 80% of the 3DS VEReq messages got a response of Y. It does not mean that more than 80% of the cards have enrolled for 3DS. It only indicates that more and more issuers are participating in stand-in services. As a result of it, you would also notice that a lot of 3DS authentications have an A (Attempted) status. Stand-in is the magic behind it!