(https://www.modirum.com/)

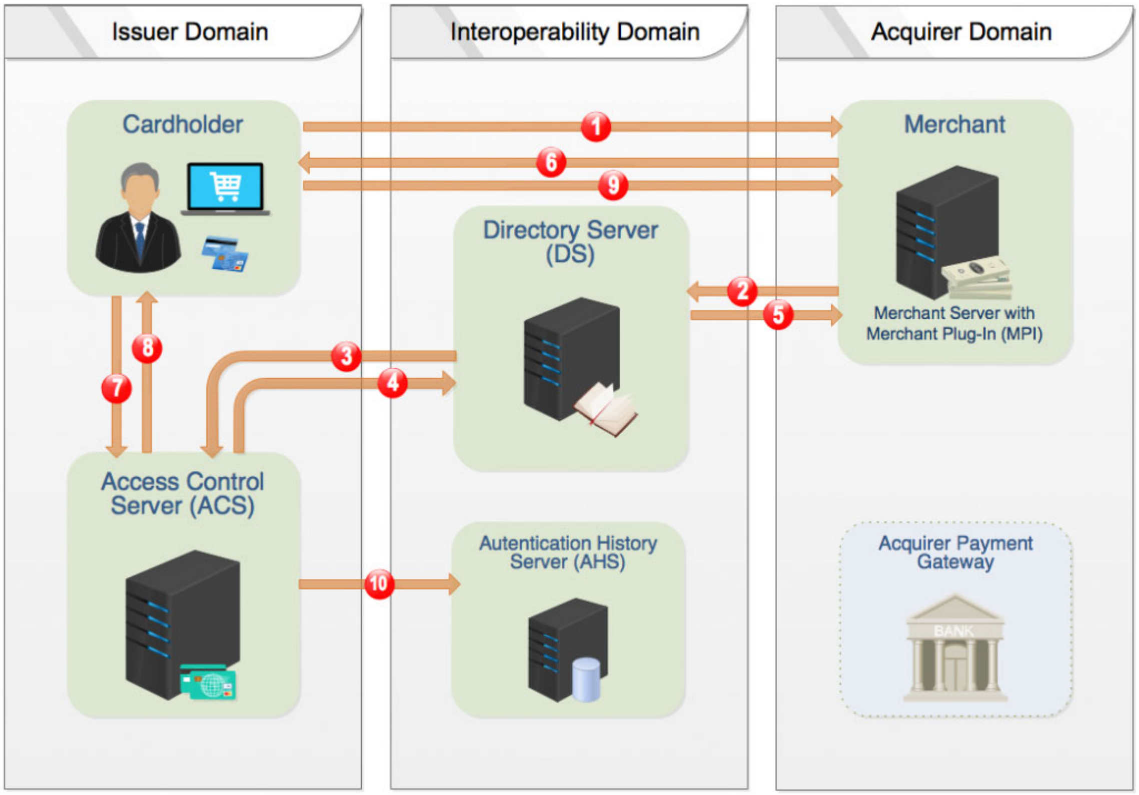
3-D Secure

Three-Domain Secure (3DS or 3-D Secure) is a XML-based messaging protocol to enable cardholders to authenticate themselves with their card issuer while making card-not-present (CNP) online purchases. 3-D Secure helps to prevent unauthorised CNP transactions and protects the merchants and issuers and cardholders from fraud on cards.

3-D Secure facilitates the exchange of cardholder data between CNP transaction participants – cardholder, merchant, card issuer and payment system. 3-D Secure version 1.0 was initially developed by Visa and marketed as Verified by Visa (VbV) since early 2000s. Services based on the 3-D Secure 1.0 have also been adopted by MasterCard as MasterCard SecureCode (MCC), by JCB International as J/Secure and by American Express as American Express SafeKey.

How 3-D Secure 1.0 works

The three domains consist of the merchant / acquirer domain, issuer domain, and the interoperability domain (e.g. payment systems). This is simplified diagram of 3-D Secure 1.0 process workflow:



(https://www.modirum.com/files/2017/05/3ds10.png)
3-D Secure 1.0 Diagram

1. The online-customer (Cardholder) in their web-browser checks-out at the merchant site and enters their payment card details.
2. If Merchant's site enables 3- D Secure, it implements the merchant plug-in (MPI). MPI contacts the Payment System Directory Server (DS) located in the Interoperability Domain to verify the enrolment of the payment card in 3-D Secure by sending to the DS a Verifying Enrolment Request (VEReq) which includes Cardholder's payment card number (primary account number (PAN)).
3. Based on the PAN, the DS finds the card issuer's Access Control Server (ACS) and contacts it to determine whether the card is enrolled in 3-D Secure.
4. The ACS responds to the DS, confirming or not confirming that card with the given PAN is enrolled in the payment system.
5. The DS responds to the MPI with a Verifying Enrolment Response (VERes) message, confirming to the MPI whether the card is enrolled or not. If card is enrolled, the VERes message include the URL of the card issuer's ACS.
6. Merchant's MPI redirects (or provides iFrame) Cardholder browser to the ACS URL adding to POST-request signed Payer Authentication Request (PAReq), which includes PAN and other transaction details.
7. The Cardholder authenticates himself at the ACS authentication. Depending on supporting authentication method it can be One Time PIN, known fixed password, login to web bank, etc. The personal assurance message (PAM) is chosen by cardholder during the enrolment maybe displayed on this page, if Issuer supports this option.
8. When Cardholder submitted authentication form as above, the ACS redirects them back to MPI adding a Payer Authentication Response (PARes) message.
9. The PARes is then forwarded to the MPI via the customer's browser. PARes includes the transaction status which indicates whether the customer has successfully authenticated with 3-D Secure. Depending on payment system rules and the transaction status in PARes message the merchant can proceed with a payment authorisation request.

3-D Secure 1.0 drawbacks.

The main benefit of 3-D Secure is shifting the possible fraud responsibility from the merchant to the card issuer, which reduces chargebacks. Nevertheless, many merchants don't use the 3-D Secure, due to that the benefit form the less chargeback does not compensate losses in conversion rates and costs of service.

Main disadvantages of version 3D-Secure 1.0 are:

- workflow might be complicated or confusing for a cardholder, which leads to smaller conversion (abandoned shopping carts problem);
- 3-D Secure 1.0 doesn't fit well with mobile devices;
- lack of seamless integration with modern payment tools like wallets;
- limited set of possible authentication methods, which some are outdated and unsafe;
- very limited ability of frictionless authorisation based on dynamic risks scoring.

3-D Secure 2.0 enhancements

Due to above mentioned drawbacks and for better reflecting current and future market requirements, the payments industry recognised the need to create a new 3-D Secure specification. Thus since January 2015, EMVCo, a company which is collectively owned by American Express, Discover, JCB, MasterCard, UnionPay and Visa, were developing the EMV 3DS 2.0 Specification and in October 2016, the specs for 3-D Secure 2.0 was published.

EMVCo declares that new specification of 3-D Secure 2.0:

- Supports specific app-based purchases on mobile and other consumer devices
- Improves the consumer experience by enabling intelligent risk-based decisioning that encourages frictionless consumer authentication
- Delivers industry leading security features
- Specifies use of multiple options for step-up authentication, including one-time passcodes, as well as biometrics via out-of-band authentication
- Enhances functionality that enables merchants to integrate the authentication process into their checkout experiences, for both app and browser-based implementations
- Offers performance improvements for end-to-end message processing
- Adds a non-payment message category to provide cardholder verification details to support various non-payment activities, such as adding a payment card to a digital wallet.

How 3-D Secure 2.0 works.

Changes in components

As 3-D Secure 2.0 has to support new authentication flows, it extends the 3-D Secure ecosystem by introducing new components and defining new terms. All components present in Acquirer (Merchant) domain now named by collective term “**3DS Requestor Environment**”.

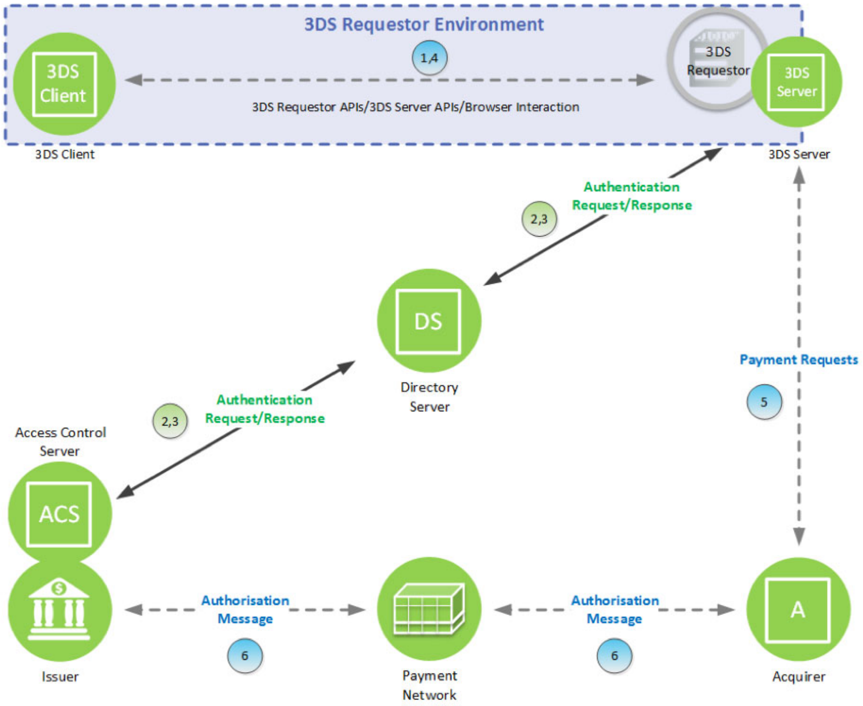
The 3DS Server - system that handles online transactions and facilitates communication between the 3DS Requestor and the DS, replaces term Merchant Server Plug-in (MPI).

3DS Client - the consumer-facing component allowing cardholder interaction with the 3DS Requestor. For example – online-shopping web application or online-shopping mobile application. This can be implemented via in-app (3DS SDK) and browser based purchases (3DS Method). Both could be integrated with the 3DS Requestor for a smooth online shopping experience.

3DS Requestor - the initiator of the 3-D Secure 2.0 authentication request (AReq). For example, this may be a merchant or a digital wallet requesting authentication within a purchase flow.

Changes in flows

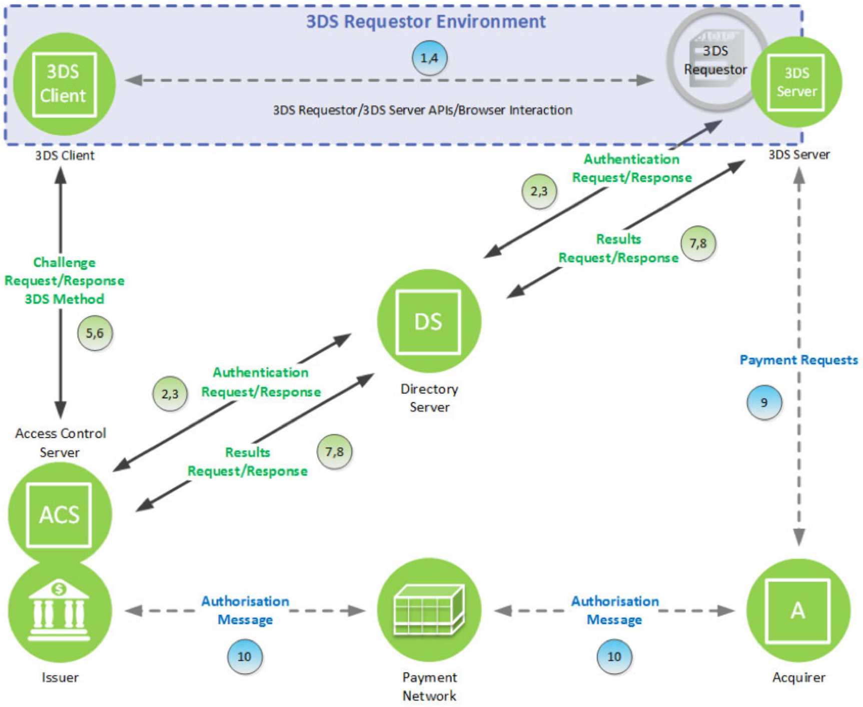
The biggest difference since 3DS 1.0 is the **Frictionless flow** which allows issuer to approve a transaction without cardholder interaction based on risk-based-authentication performed in the ACS. (Steps 1-4 at the figure below)



Note: Dashed arrows and 3DS Requestor are not part of 3DS specification and are shown for clarity only

(http://www.modirum.com/files/2017/05/3ds20.png)

Challenge flow has got changed way of communication from the Issuer to Merchant. In 3DS 2.0 the result of challenge is communicated through the DS. (Step 6 at the figure below) Thus, Merchant is informed about the authentication results via a separate channel, which is more secure.



Note: Dashed arrows and 3DS Requestor are not part of 3DS specification and are shown for clarity only

(http://www.modirum.com/files/2017/05/3ds20-challenge.png)

Non-payment Authentication - 3-D Secure 2.0 also introduces special non-payment customer authentication, which can be used for cardholder Identification & Verification (ID&V) for mobile wallets and the secure request of tokens for card on file. This flow is similar to the 3-D Secure 2.0 authentication flow during a purchase on the web shop, but it does not include payment specific steps like payment initiation, confirmation etc.

Changes in messages

Comparing 3DS 1.0 version 2.0 introduces new messages and change the names for the messages that are exchanged between the components. A new message type is the Result message (RReq and RRes), which is exchanged between the Issuer (ACS) and the Merchant (3DS Server) to communicates the result after cardholder verification.

New data fields were added to messages to support new functionalities. Also, 3-D Secure 2.0 defines messages with JSON, compared to XML in version 1.0.

This table illustrates changes in messages:

3DS Transaction Phase	3DS 1.0	3DS 2.x
Ranges cache loading	CRReq/CRRes	PReq/Pres (Preparation Message)
Participation/enrollment check	VEReq/VERes	AReq/ARes (Authentication Message)
Frictionless authentication	N/A	Part of AReq/ARes
Challenge authentication and confirmation	PAReq/PARes	CReq/CRes (Challenge Message) + RReq/RRes (Results confirmation Message)

Changes in Authentication Methods

3-D Secure 2.0 makes deprecated the following authentication methods, which are not considered to be secure:

- Fixed or Static passwords including random static passwords
- Printed OTP cards, Bingo or Transaction Authentication Number (TAN) cards
- Delivery of one-time password (OTP) via ATM
- Knowledge based questions/KB rules

They are not allowed for Primary or Fall-back Authentication.

- Redirection flow is allowed to use in 3-D Secure 2.0 only in iFrame's

New or expanded authentication options:

Risk-based Authentication

Risk-based Authentication (RBA) becomes a highly recommended to be used.

Usage of RBA is the mechanism, which allows Issuer to implement frictionless payments for low risk transactions. That requires issuer to have risk engine implemented and appropriately configured set of risk rules created. Issuers may implement own RBA algorithm or use independent vendors for such risk engine implementation – like Fraud Scoring Server (FSS) from Modirum.

Biometric authentication

Using of biometric authentication devices and flows become also a highly recommended by payment systems. This technology is becoming mature enough to provide good security and performance level, as well as positive consumer experience at checkout. Available methods are fingerprint match, voice and facial recognition.

Support for Mobile devices

Support of Mobile devices is mandatory with 3-D Secure 2.0. Any used authentication flow should grant support for mobile devices. That means all authentication flows, which do not provide it will not be granted with 3-D Secure 2.0 certification by EMVCo nor by payment systems.

Methods existed in 3-D Secure 1.0 and still valid for using with 3-D Secure 2.0 are:

Out-Of-Band

The Out-Of-Band authentication means usage of two different channels or two factors in verification process. Both of them should be applicable for in 3-D Secure 2.0. For example, primary authentication may be passed by voice or facial recognition, while secondary pass may be granted with SMS OTP.

Redirection

The only browser redirection can be used with 3-D Secure 2.0. Obsolete native (application) redirection should be replaced by other appropriate authentication method. Browser redirection authentication according 3-D Secure 2.0 has to support mobile devices and be able to work in iFrame.

Background Authentication

In Background authentication method ACS is working as a proxy server. It forwards both PAReq and VEReq messages to the issuer's background server instead of processing them. This approach is fine from 3-D Secure 2.0 perspective if issuer implements a proper authentication method.

Current status and future of 3-D Secure

EMVCo published the EMV® 3-D Secure – Protocol and Core Functions Specification version 2.0 in October 2016 and EMV® 3-D Secure – SDK Specification in January 2017.

Currently drafts of the next versions of the documents are being discussed.

At Q3-Q4 2017 EMV® 3-D Secure 2.0 certification for software and service vendors should become available.

Payment systems defines their own certification requirements for 3-D Secure 2.0. MasterCard already updated their MasterCard Identity Check program for 3-D Secure 2.0. Visa should publish their requirement in closest time.

Since EMVCo certification details are yet unavailable, it is still expected that 3-D Secure 2.0 needs to be implemented during 2018. 3-D Secure 1.0 will not be supported as of 1.1.2020.