wirecard

3D SECURE

We have seen merchants reduce fraud by up to 95% when integrating to 3D Secure....

System Overview

This document is intended for merchant and developers that want to gain a high level overview and understanding of integrating to Wirecard's 3D Secure service.

CONTENTS

Overview **3**
What is 3D Secure? 3
3D Secure Architecture **3**
Three Domain Model 4
3-D Secure Entities 4
How Payment Authentication Works 6
3D-Secure Transactional Process **7**
High Level 3D Secure Transaction Process 7
3D Secure Transaction Flow Diagram **9**
Wirecard's Role in 3D Secure **10**
Developers Integration Role in 3D Secure **10**
My Virtual Solution 10
My Enterprise Solution 10
Merchants Role in 3D Secure **10**
Reducing Risk **10**
Reporting **10**
Understanding Electronic Commerce Indicators (ECI) **11**
Understanding Transaction Status **11**
ECI & Transaction Status Matrix **11**
Card Holder 3D Secure Scenarios – My Enterprise Solution **12**
Scenario 1 – Cardholder is registered for 3D-Secure: 12
Scenario 2 - Card Holder is NOT registered for 3D-Secure and their bank requires them to register 12
Scenario 3 - Card Holder is NOT registered for 3D-Secure and their bank does NOT require them to 12
Scenario 4 – Issuing Bank does not Participate in 3D Secure 13
3D Secure Terminology **13**

Overview

Internet transactions are classed as 'cardholder not present' (CNP) transactions. 3D Secure helps to identify a cardholder and confirm that it was indeed the legitimate cardholder entering the card details, ensuring safe online transactions through Wirecard's Payment Services.

The majority of chargebacks can arise as a result of the cardholder denying that they authorized a transaction, making it difficult for you to successfully dispute this sort of chargeback. The 3D Secure technology is designed to reduce the possibility of fraudulent card use by authenticating the cardholder at the actual time of the transaction and subsequently reducing your exposure to disputed transactions and chargebacks of this type.

What is 3D Secure?

3D Secure stands for Three Domain Secure - the payment industry's internet authentication standard which has been developed by the major card schemes. Visa has called their version of the scheme 'Verified by Visa' and MasterCard have called their equivalent initiative 'MasterCard SecureCode'. These are both collectively referred to as 3D Secure.

3D Secure authentication requires the cardholder to register their card to take advantage of this service. This is a onetime process which takes place on the card issuer's website and involves the cardholder answering several security questions to which only the card issuer and cardholder will know the answer. The cardholder selects a password and agrees on a secret phrase, which will be used by the card issuer during each online transaction.

3D Secure can be thought of as an online version of 'Chip and Pin' technology, whereby the cardholder has a personalized password registered with their card that is entered during the checkout process. 3D Secure is predicted to become the industry standard and all online consumers will soon become as familiar with this, as when they enter their 'Pin' number at a cash machine or till in a shop.

3D Secure Architecture

Purpose	This section describes the Three Domain Model within which the entities involved in 3D Secure work together to authenticate and authorize an online payment transaction. The role of each entity is described and as simple transaction diagram shows the messages that move among them.
Organization	This section includes the following topics:

Topic
Three Domain Model
3-D Secure Entities
How Payment Authentication Works
Purchase Transaction Flow

Three Domain Model

The domains

Visa and MasterCard has developed the Three Domain Model of payment systems as the basis of new payment solutions. The model divides payment systems as follows:

Domain	Description
Issuer Domain	Systems and functions of the issuer and its customers (cardholders)
Acquirer Domain	Systems and functions of the acquirer and its customers (merchants)
Interoperability Domain	Systems, functions, and messages that allow Issuer Domain systems and Acquirer Domain systems to interoperate worldwide

The model

The Three Domain Model enables issuers to authenticate their cardholders during online purchases. Interoperability between the issuer and acquirer is achieved through the use of a common protocol and the Visa / MasterCard interoperability services.

3-D Secure in Three Domain Model

- Messages to request and receive the results of authentication flow between the acquirer and the Issuer Domains within the Interoperability domain via the Internet.
- Messages to perform cardholder authentication flow between the cardholder and the issuer within the Issuer Domain.
- Messages to request authorization and payment processing flow between the merchant and the acquirer within the Acquirer Domain.
- Messages to perform authorization and payment processing flow between the acquirer and the issuer within the Interoperability domain via VisaNet.

3-D Secure Entities

Overview

This section describes entities that participate in 3-D Secure, by domain.

Many of the systems in the issuer and Acquirer Domains may be provided, operated, or both by third parties on behalf of Visa Members.

Issuer Domain

The entities residing in the Issuer Domain are:

Entity	Description
Cardholder	The cardholder shops online, providing the account holder name, card number, and expiration date, either directly or via software such as a digital wallet, then indicates readiness to finalize the transaction. In response to the Purchase Authentication Page, the cardholder provides information needed for authentication, such as a password.
Cardholder browser	The cardholder browser acts as a conduit to transport messages between the Merchant Server Plug-in (in the Acquirer Domain) and the Access Control Server (in the Issuer Domain).

Additional cardholder components	Optional cardholder hardware and software may supplement the abilities of the browser. For example, chip card implementations will require additional cardholder software and a card reader. Implementations which achieve cardholder authentication via password should not require any additions to cardholder hardware or software.
Issuer	A Visa Member financial institution that: • Enters into a contractual relationship with the cardholder for issuance of one or more Visa cards • Determines the cardholder's eligibility to participate in 3-D Secure • Defines card number ranges eligible to participate in 3-D Secure • Provides data about those card number ranges to the Directory Server and to the ACS performs enrolment of the cardholder for each payment card account (via the Access Control Server, a separate Enrolment Server, or manually)
Access Control Server	The Access Control Server (ACS) has two functions: • To verify whether a given card number is enrolled in 3-D Secure and whether authentication is available • To authenticate the cardholder for a specific transaction Although these functions are described as belonging to a single logical ACS, implementations may divide the processing by function or by other characteristics such as card number range among multiple physical servers.

Acquirer Domain The entities residing in the Acquirer Domain are:

Entity	Description
Merchant	Existing merchant software handles the shopping experience, obtains the card number, then invokes the Merchant Server Plug-in to conduct payment authentication. If payment authentication is successful, the merchant software submits an authorization request to the acquirer.
Merchant Server Plug-in	The Merchant Server Plug-in (MPI) creates and processes payment authentication messages, then returns control to the merchant software. As part of processing the authentication response message from the issuer, the MPI may validate the digital signature in the message; alternatively, this function may be performed by a separate server, or by the acquirer or a third party.
Acquirer	A financial institution that: • Enters into a contractual relationship with a merchant for purposes of accepting cards • Determines the merchant's eligibility to participate in 3-D Secure Following payment authentication, the acquirer performs its traditional role: • Receives authorization requests from the merchant • Forwards them to the authorization system (such as VisaNet) • Provides authorization responses to the merchant • Submits the completed transaction to the settlement system (such as VisaNet)

Interoperability Domain The entities residing in the Interoperability domain are:

Entity	Description

Directory Server	The Directory Server: • Receives messages from Merchant Plug-In servers querying a specific card number • Determines whether the card number is in a participating card range • Directs the request for cardholder authentication to the appropriate ACS (in the Issuer Domain) or responds directly to the merchant • Receives the response from the ACS indicating whether payment authentication is available for the cardholder account • Forwards the response to the merchant
Commercial Certificate Authority	Generates the following kind of certificates for the use of 3-D Secure entities: • SSL/TLS client and server certificates
Certificate Authority	Generates selected certificates for the use of 3-D Secure entities, including: • Signing certificates • Visa Root certificate
Authentication History Server	The Authentication History Server, operated by Visa: • Receives a message from the ACS for each attempted payment authentication (whether or not authentication was successful) • Stores the records received A copy of the data stored by the Authentication History Server is available to acquirers and issuers in case of disputes.
VisaNet	Following payment authentication, VisaNet performs its traditional role: • Receives authorization requests from the acquirer • Forwards them to the issuer • Provides responses from the issuer to the acquirer • Provides clearing and settlement services to the acquirer and issuer

How Payment Authentication Works

Overview

This section provides a high-level narrative outline of the major steps in a 3-D Secure payment authentication.

The section that follows provides more detail about messages and control flows.

Cardholder purchase

When checking out at the conclusion of shopping, cardholder supplies billing and payment card information, or uses merchant capabilities or software such as a digital wallet to do this. When the cardholder indicates the decision to buy, Merchant Server Plug-in (MPI) software is activated. MPI software is typically located at the acquirer or at a third-party processor site. In other regions, such as the USA, the MPI may be located at the shopping site of large merchants.

Request to Directory Server	The MPI sends a message to the Directory Server to determine whether authentication services are available for the cardholder. • If the response indicates that the cardholder is enrolled and authentication is available, the response message instructs the MPI how to contact the Access Control Server (ACS) of the associated issuer. • If the response indicates that the cardholder is not enrolled or authentication is otherwise not available, the merchant storefront application handles the purchase as a non-authenticated purchase.
Cardholder authentication	The MPI sends an authentication request to the ACS. This is usually sent via the cardholder browser. The ACS authenticates the cardholder by causing an authentication dialog to be displayed to the cardholder asking for password, or by some other authentication method. The ACS formats and digitally signs the authentication response, then returns it to the MPI.
Payment processing	If the authentication response indicates successful authentication, the merchant sends a traditional payment authorization request to its acquirer. Depending on regional requirements, the authorization request may include additional data such as the Electronic Commerce Indicator (ECI) and other transaction data.

3D-Secure Transactional Process

The 3D Secure process consists of a web service call followed by a form post. Each call can bring back variable results that will form part of the next process.

High Level 3D Secure Transaction Process:

Step 1 - Shopper browses at merchant site, adds items to shopping cart, then finalizes purchase.
Step 2 - The merchant will invoke a web service (CMPI Lookup Request) to the Wirecard's Merchant Programming Interface (MPI) with the necessary data to begin the 3D Secure processing including card number.
Step 3 - The Wirecard MPI sends query including card number to Directory Server. This is the VERes.
Step 4 - If card number is in a participating card range, Directory Server queries appropriate Access Control Server (ACS) to determine whether card number is enrolled.
Step 5 - ACS responds to Directory Server, indicating whether authentication is available for the card number.
Step 6 - Directory Server forwards ACS response (or its own) to Wirecard MPI.
Step 7 - Wirecard's MPI will return a CMPI Lookup Result to the merchant. If cardholder is not enrolled in 3D Secure or if authentication is otherwise unavailable, the merchant submits a traditional authorization request and processing ends.
Step 8 - Based on the result (issuer or card type participating), merchant initiates a form post (ACS Request) that posts the values retrieved from the CMPI Lookup Result (first web service call) to the Access Control Server (ACS) via the shopper's browser.
Step 9 - ACS authenticates shopper as appropriate for the card number then formats the ACS Result message with appropriate values and digitally signs it.
Step 10a - ACS returns a ACS result (PARes) to merchant via shopper's browser.
Step 10b - ACS sends a copy of the Payer Authentication Response to the Authentication History Server.

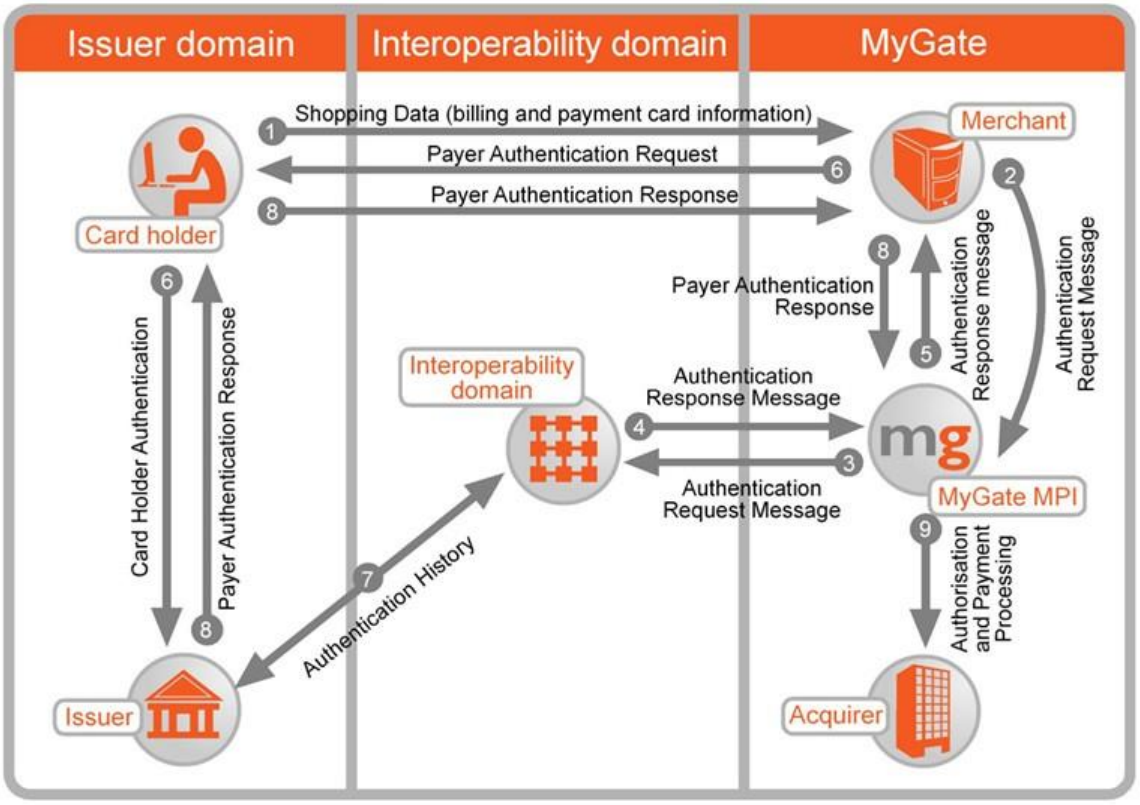
Step 11 -The merchant will invoke a web service (CMPI Authenticate Request) to the Wirecard's with the PARes and 3D Secure Transaction ID.

Step 12 –Wirecard will return the 3D Secure data elements (PARes Status, Signature Verification, ECI, XID and CAVV) for the merchant to store for evidence.

Step 13 - Merchant process the result with authorization request to Wirecard MPI.

Step 14 - Wirecard MPI validates Payer Authentication Response signature. If successful, the Wirecard proceeds with authorization exchange with acquirer / bank.

3D Secure Transaction Flow Diagram



Wirecard's Role in 3D Secure

Wirecard's payment platform is integrated to the MPI (merchant programming interface) enabling transactions to be processed to both the MasterCard Secure Code & Verified by Visa, 3D Secure schemes.

1. Each time a cardholder attempts to make a transaction using Wirecard, after entering their personal card details on the Wirecard payment page, Wirecard automatically checks to see if their card is enrolled in the 3D Secure scheme by calling the Directory Server.
2. If the cardholder's bank is participating, the cardholder is taken to their card issuers secure website (Access Control Server) where they enter their 3D Secure password. The payment is then processed to the acquirer and the cardholder is smoothly delivered back to the merchants confirmation page.
3. If a cardholder of a bank who is participating in the 3D Secure scheme has not yet enrolled, by default, the issuer may prompt the cardholder to register. The cardholder can then enrol their card with 3D. Different card issuers may implement a maximum decline limit before the cardholder is made to sign up to 3D Secure.
4. Wirecard will attempt a 3D Secure check on each card transaction - if the cardholder's bank are not currently participating in the 3D Secure scheme, the transaction will process directly to the acquirer.

Developers Integration Role in 3D Secure

My Virtual Solution

If you are integrating to the My Virtual solution, you will not be required to integrate to the 3D Secure service as My Virtual will handle entire the 3D Secure process once it has received the form post..

My Enterprise Solution

If you are integrating to the My Enterprise solution you will be required to integrate to a component of the 3D Secure process whereby Wirecard will send the request to the MPI and return the result to the merchant's web server whereby the merchant may be required, based on the MPI result to call the ACS server for card holder authentication and return the result back to Wirecard.

Merchants Role in 3D Secure

A merchant must request that their merchant account be 3D Secure enabled.

Reducing Risk

Merchants can request that Wirecard configure transactions with an ECI indicator of Visa – 7 or MasterCard – 0 to be blocked from processing as these indicators show that the MPI returned a Transaction Status - U (Undefined) meaning that the liability shift will remain with the merchant.

Reporting

Merchants can view the ECI status of a transaction from the Transaction Report within the Wirecard Web Console.

wirecard

Understanding Electronic Commerce Indicators (ECI)

The ECI indicates the security level associated with an Internet purchase transaction.
The ACS will return an ECI in the message which the merchant can use to gauge risk associated with the transaction. The payment gateway will process the ECI to the acquirer or its processor for inclusion in the authorization request message.

Note: Refer to the ECI & Transaction Matrix for ECI values and risks associated them.

Note: Some ECI indicators will allow liability shift for certain transactions relating to chargebacks.

Note: Merchants can request that Wirecard block specific ECI's that do not allow for liability shift.

Understanding Transaction Status

The transaction status is an alpa character relating to payment authentication results. After completing a successful validation of the issuer's digital signature using the Root Certificate, the MPI reviews the value in the Transaction Status field of the PARes to determine the payment authentication results (authentication successful or authentication failed) and proceeds with the authorization as illustrated in the ECI Matrix below.

ECI & Transaction Status Matrix

The below diagram illustrates the different scenarios.

ECI	Transaction Status	Authentication attempt results	Merchant response	Action
MasterCard - 2 **Visa – 5**	**Y**	**Successful** cardholder authentication.	**Successful 3-D Secure processing.** The ACS returns the transaction and the authentication data (CAVV, ECI and XID) necessary to build a 3D Secure authorization request.	**Liability Shift**
MasterCard - 1 **Visa – 6**	**A**	**Proof of Attempt** occurred and authentication could not be performed.		
N/A	**N**	**Failed** cardholder authentication.	**Suspicious Transaction** The ACS returns the transaction and data to the merchant informing them to disallow the purchase. Merchants are not permitted to submit transactions where the cardholder failed payment authentication. Merchants may wish to ask the customer for another form of payment.	**No Liability Shift**
MasterCard - 0 **Visa – 7**	**U**	**ACS unable** or unavailable to perform payment authentication.	**Exception Processing** The ACS returns the transaction and ECI data necessary to build, due to a processing exception, merchant can continue processing but with **no liability shift.**	**No Liability Shift**
	n/a	**ACS processing error** occurred and authentication could not be performed.		

Note: The above tables are based on interpretation of Visa and MasterCard specifications and in no way can Wirecard guarantee the liability shift to the merchant by the acquirer. For more information on liability shift please refer to Visa and MasterCard policies or speak to your acquirer.

Card Holder 3D Secure Scenarios – My Enterprise Solution

The below describes different 3D Secure processing scenarios if you are using the My Enterprise Solution:

Note: My Virtual handles the entire 3D Secure process and no integration is required.

Scenario 1 – Cardholder is registered for 3D-Secure:

1. The cardholder will come onto the merchants website and chooses a product.
2. The card holder clicks on “Checkout” and goes to the payment page.
3. The card holder enters their card details and click on “Process” or “Pay Now”.
4. A web service is invoked to the Wirecard 3D-Secure service which will call the director server.
5. If the cardholder’s bank (issuer) is participating, Wirecard will post to the merchant the URL that the cardholder is to be redirected to (Access Control Server) where the card holder can enter their 3D Secure password.
6. When the cardholder has completed entering their password, the Access Control Server will redirect the cardholder back to the merchant website with the 3D-Secure results and these variables are populated in the web service code for the authorization request.
7. Wirecard will then process the authorization request to the acquirer and the cardholder is smoothly delivered back to the merchants confirmation page.

Scenario 2 - Card Holder is NOT registered for 3D-Secure and their bank requires them to register:

1. The card holder will come onto the merchant’s website and chooses a product.
2. The card holder clicks on “Checkout” and goes to the payment page.
3. The card holder enters their card details and click on “Process” or “Pay Now”.
4. A web service is invoked to the Wirecard 3D-Secure service which will call the director server.
5. If the cardholder’s bank (issuer) is participating, Wirecard will post to the merchant the URL that the cardholder is to be redirected to (Access Control Server) where the card holder can complete 3D Secure enrolment.
6. The card holder will need to enter their card number, ID number and create a password (This is their 3D-Secure PIN that they will use in 3D Secure future transactions).
7. When the cardholder has completed registration, the Access Control Server will redirect the cardholder back to the merchant website with the 3D-Secure results and these variables are populated in the web service code for the authorization request.
8. Wirecard will then process the authorization request to the acquirer and the cardholder is smoothly delivered back to the merchants confirmation page.

Scenario 3 - Card Holder is NOT registered for 3D-Secure and their bank does NOT require them to:

1. The card holder will come onto the merchants website and chooses a product.
2. The card holder clicks on “Checkout” and goes to the payment page.

3. The card holder enters their card details and click on “Process” or “Pay Now”.
4. A web service is invoked to the Wirecard 3D-Secure service which will call the director server.
9. If the cardholder’s bank (issuer) is participating but the cardholder is NOT, Wirecard will post to the merchant the 3D-Secure results from the director server and these variables are populated in the web service code for the authorization request.
5. This result is populated in your web service code and the transaction can continue.
6. Wirecard will then process the authorization request to the acquirer and the cardholder is smoothly delivered back to the merchants confirmation page.

Scenario 4 – Issuing Bank does not Participate in 3D Secure:

1. The card holder will come onto the merchants website and chooses a product.
2. The card holder clicks on “Checkout” and goes to the payment page.
3. The card holder enters their card details and click on “Process” or “Pay Now”.
4. A web service is invoked to the Wirecard 3D-Secure service which will call the director server.
5. If the cardholder’s bank (issuer) is NOT participating, Wirecard will post to the merchant the 3D-Secure results from the directory server and these variables are populated in the web service code for the authorization request.
6. This result is populated in your web service code and the transaction can continue.
7. Wirecard will then process the authorization request to the acquirer and the cardholder is smoothly delivered back to the merchant’s confirmation page.

Note: Only the card holder knows their 3D Secure PIN. In the event that the card holder does not know their password, they would need to contact their banks 3D-Secure department to have their PIN reset.

3D Secure Terminology

TERM	DESCRIPTION
3 D Secure	An e commerce protocol that enables the secure processing of payment card transactions over the Internet; one of the supported protocols of the Visa Authenticated Payment Program.
Access Control Server (ACS)	A database of cardholders enrolled in 3 D Secure, containing cardholder account and password information. It is operated by the card issuer or by Visa on behalf of the issuer. In response to merchant/Directory Server inquiries, it verifies cardholder enrolment in 3 D Secure; receives authentication requests from merchants and authenticates the cardholder during online purchases; and provides digitally-signed authentication response messages containing the authentication results and other 3 D Secure data to the merchant and the Authentication History Server.
Account Information Security Program	One of the programs of the Visa Secure e commerce Initiative, establishes standards for e commerce merchants to help them ensure that cardholder data is secure at their sites
Acquirer	A Visa Association financial institution that establishes a contractual service relationship with a merchant for the purpose of accepting Visa cards. Also determines whether merchant is eligible to participate in 3 D Secure. Performs traditional role of receiving and forwarding authorization and settlement messages (enters transaction into interchange).
Acquirer Domain	Contains the systems and functions of the acquirer and its customers, such as merchants
ACS	See Access Control Server
AID	Application Identifier
Authentication	The process of verifying that the person making an e commerce purchase is entitled to use the payment card.
Authentication History Server (AHS)	A component that operates in the Interoperability domain; archives authentication activity for use by acquirers and issuers for dispute resolution and other purposes.
Authorization	The process in which the issuer, or a processor on the issuer's behalf, approves or denies a Visa card transaction.

Authorization Request Cryptogram	The cryptogram generated by a chip card for transactions requiring online authorization, sent to the issuer for validation.
Bank Identification Number (BIN)	The first 6 digits of a payment card account number which uniquely identify the issuing financial institution.
BIN	See Bank Identification Number
Browser	A client program that allows users to read hypertext documents on the World Wide Web and navigate between them. Examples are Netscape Navigator and Microsoft Internet Explorer.
Cardholder	An individual to whom a credit card is issued by a Visa Member issuer.
Cardholder Authentication Verification Value	A cryptographic value generated by the ACS to provide a way during authorization processing for VisaNet to rapidly validate the integrity of certain values copied from the Payer Authentication Response to the authorization request and to prove that authentication occurred.
Cardholder Browser	Acts as a conduit to transport messages between the Merchant Server Plug-in (in the Acquirer domain) and the Access Control Server (in the Issuer Domain).
CAVV	Cardholder Authentication Verification Value
Certificate	An electronic document that contains the public key of the certificate holder and which is attested to by a certificate authority and rendered unforgettable by cryptographic technology (signing with the private key of the certificate authority).
Cryptography	The process of protecting information by transforming it into an unreadable format. The information is encrypted using a key, which makes the data unreadable, and is later decrypted when the information needs to be used again.
Digital Signature	An asymmetric cryptographic method whereby the recipient of the data can prove the origin and integrity of data, thereby protecting the sender of the data and the recipient against modification or forgery by third parties and the sender against forgery by the recipient. Contrast with Message Authentication Code.
Enrolment Server	Operates in the Issuer Domain; a server hardware/software entity which manages cardholder enrolment in 3 D Secure by presenting a series of questions via a Web interface to be answered by the cardholder and verified by the issuer.
Interoperability Domain	Facilitates the transfer of information between the issuer and Acquirer domain systems.
Issuer	A Visa Member financial institution that enters into a contractual relationship with the cardholder for issuance of one or more Visa cards and determines the eligibility of the cardholder to participate in 3 D Secure.
Issuer Domain	Contains the systems and functions of the issuer and its customers
Key	In cryptography, the value needed to encrypt and/or decrypt something.
Key Management	The handling of cryptographic keys and other security parameters during the entire lifetime of the keys, including generation, storage, entry and use, deletion or destruction, and archiving.
Merchant	An entity that contracts with a Visa acquirer to originate transactions and that accepts payment cards. All Visa merchants must have a contractual relationship with a Visa acquirer.
Merchant Commerce Server	A server hardware/software entity which handles online transactions and facilitates communication between the merchant application and the Visa gateway.
Merchant Server Plug (MPI)	Operates in the acquirer domain; a component that is incorporated into the merchant's Web storefront that performs functions related to 3 D Secure on behalf of the merchant, such as validating the digital signature in a 3 D Secure message and determining whether a card number is enrolled in 3 D Secure.
Merchant Server Plug-In	Operates in the acquirer domain; a component that is incorporated into the merchant's Web storefront that performs functions related to 3 D Secure on behalf of the merchant, such as validating the digital signature in a 3 D Secure message and determining whether a card number is enrolled in 3 D Secure.
Message Authentication Code	A symmetric (secret key) cryptographic method that protects the sender and recipient against modification and forgery of data by third parties. Contrast with digital signature.
MPI	See Merchant Server Plug-in
PAReq	See Payer Authentication Request
Pares	See Payer Authentication Response
PATransReq	Payer Authentication Transaction Request (sent to the Authentication History Server)
PATransRes	Payer Authentication Transaction Response

Payer Authentication Request (PAReq)	A message sent from the MPI to the issuer Access Control Server via the cardholder browser. The message requests the issuer to authenticate its cardholder and contains the cardholder, merchant, and transaction-specific information necessary to do so.
Payer Authentication Response (Pares)	A message formatted, digitally signed, and sent from the issuer Access Control Server to the Merchant Server Plug-in (via the cardholder browser) providing the results of the issuer's 3 D Secure cardholder authentication.
Payment Gateway	A third party that provides an interface between the merchant/Acquirer's payment system and VisaNet.
PKI	Public Key Infrastructure
Secure Sockets Layer (SSL)	A cryptographic protocol developed to confidentially transmit information over open networks like the Internet.
SET	SET Secure Electronic Transaction™, one of the two protocols approved for the Authenticated Payment Program
SSL	See Secure Sockets Layer
Three-Domain (3-D) Secure	An e commerce protocol that enables the secure processing of transactions over the Internet.
Three-Domain Secure	See 3 D Secure.
Validation	Usually refers to validating the cryptographic signature passed in the message from the ACS to the merchant.
Validation Server	A server hardware/software entity which verifies the digital signature used by the issuer to sign the Payer Authentication response message sent to the merchant, and which may be operated by the merchant, the acquirer, or a third party. This functionality may also be included in the Merchant Server Plug-in, thus eliminating the need for a separate validation server.
VEReq	See Verify Enrolment Request
VERes	See Verify Enrolment Response
Verify Enrolment Request	Message from Merchant Server Plug-in to the Directory Server or from Directory Server to ACS, asking whether a particular card number is enrolled in 3 D Secure
Verify Enrolment Response	Message from ACS to Directory Server or Directory Server to Merchant Server Plug-in, verifying enrolment
Visa Certificate Authority	Operates in the Interoperability domain; generates and distributes selected digital certificates to entities participating in 3 D Secure.
Directory Server	A server hardware/software entity which is operated by Visa in the Interoperability Domain, to route authentication requests from merchants to specific Access Control Servers.
XML	Extensible Markup Language, a computer programming language that can serve as an extension of HTML. It is especially useful for defining elements that may not have specific HTML tag definitions.