

<u>Version</u>	<u>Date</u>	<u>Author</u>	<u>Comments</u>
1.1	15.07.2009	CQR Payment Solutions GmbH	3D Secure™ Protocol for Visa and MasterCard

Table of Contents

1	Introduction.....	3
1.1	Intended Audience	3
1.2	Terminology	3
2	Overview	4
2.1	Background.....	4
2.2	Implementation	5
3	Benefits.....	8
4	Further Reading.....	9
Appendix 1: Sample Authorization Pages.....		10
4.1	Verified by Visa.....	10
4.2	MasterCard SecureCode.....	11

1 Introduction

1.1 Intended Audience

This document is written for those who wish to learn more about the 3-D Secure™ protocol, implemented via a Merchant Server Plug-In solution to CQR's system. This document gives an overview of the service provided and the advantages of implementation from the perspective of Users and Merchants.

1.2 Terminology

- Acquirer: A financial institution which receives payment card transactions from Users on behalf of a given Merchant.
- Issuer: A financial institution which distributes payment cards and extends credit/financial services to Users.
- Merchant: A business entity which provides a product/service within a specific product category/industry, under one or more brands.
- Payment: The basic transaction representation in the CQR system. Each Payment is triggered by a User and concluded either with a cancellation or with the transfer of funds from one entity to another.
- State: Each Payment moves through a series of States as it progresses from initial request to execution, each of which represents the current status of the transaction.
- User: A third party, either an individual or representative or an organization, who wishes to obtain a product or service from a specific Shop. Users are associated with a merchant, not a shop, in the CQR system. Also known as the "customer".

2 Overview

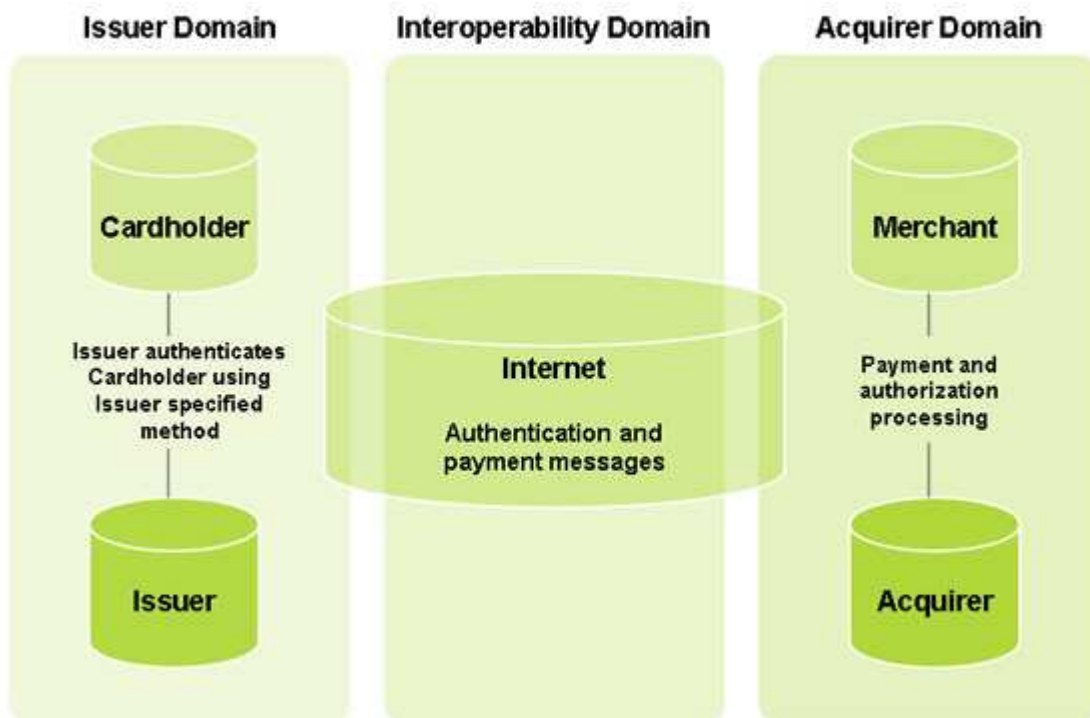
2.1 Background

The 3-D Secure™ protocol was developed and implemented by leading card networks Visa and MasterCard, who branded their service “Verified by Visa” and “MasterCard SecureCode” respectively.

The motivation for implementing this new level of transaction security was the desire to lessen the risk experienced by all parties (Merchant, User and Issuer/Acquirer) of card-not-present transactions. As the name implies, these transactions, usually completed online, are completed without the added security benefit of the card’s physical presence at the point of sale, and additionally lack the cardholder’s signature authorizing the transaction. This relative dearth of security measures facilitated fraudulent activity and exposed online Merchants to a higher risk of chargebacks and Users to the danger of unauthorized transactions.

The 3-D Secure™ protocol (named for the Three Domains of online card transactions: Issuer, Acquirer and Interoperability/Internet/Settlement Network) addresses this issue by ensuring that participating cards may only be used in a card-not-present environment if a correct password or other identity verifying information is provided for that card upon authorization – an identifier selected by the registered owner of the card upon registration with the service.

Below is a visual representation of the three domains of 3-D Secure™ as provided by Visa:

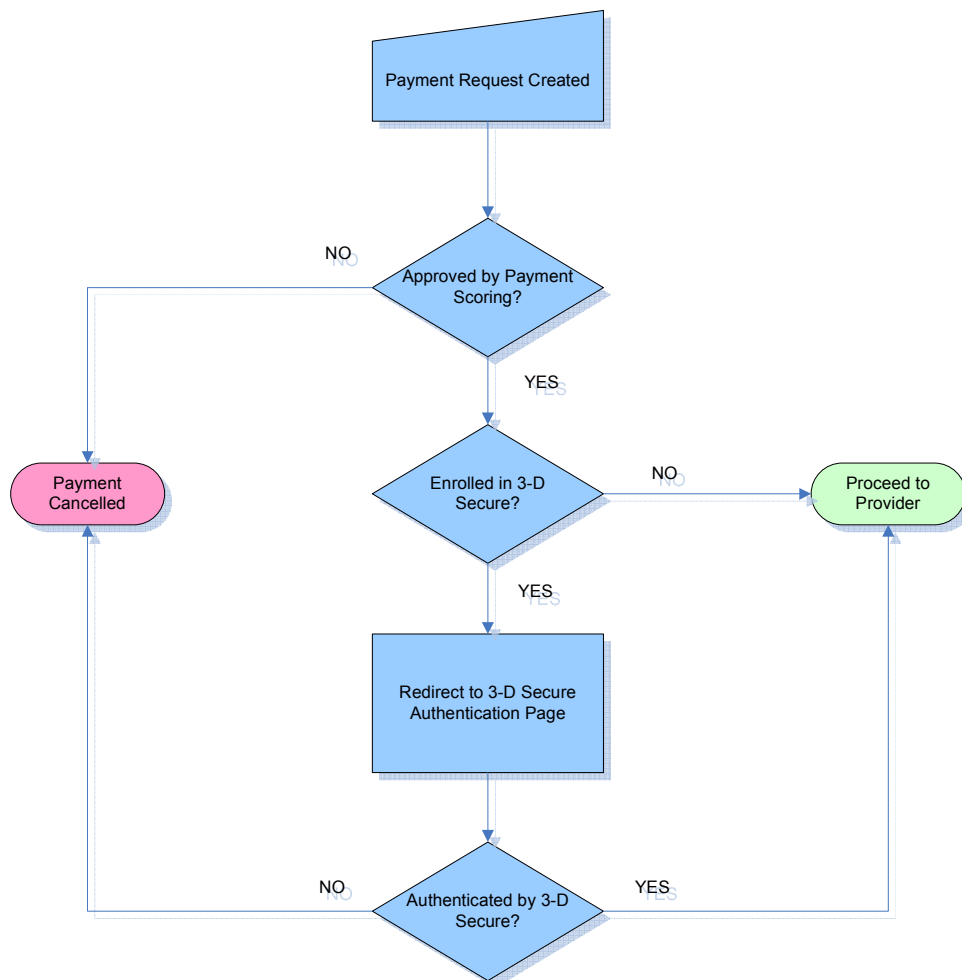


Note that the task of authenticating a User is undertaken by the Issuer, that of processing and executing the request is performed by the Merchant and Acquirer, while communication takes place across the Internet and is supervised by the payment network (in this case, Visa).

Finally, all information transferred between parties during the process of authentication and authorization takes place using Secure Sockets Layer (SSL) encryption in order to ensure maximum protection of sensitive card data.

2.2 Implementation

The 3-D Secure™ authentication check, while similar in purpose to other security checks implemented within the CQR system, is not executed by the Payment Scoring Platform. Instead, it is part of the Payment authorization process, and as such the process is defined by a series of States. A basic representation of the process is shown below:



The authentication process begins when the User submits their credit card or Maestro debit card information to the Merchant/CQR upon initiating a Payment request. At this point, a query of the relevant network's database is made by CQR in order to determine if this card is enrolled in the Verified by Visa/MasterCard SecureCode program. Currently, only card transactions processed by Acquirer Streamline are subject to the 3-D Secure™ check.

If the card is registered, the User is then redirected to an authorization site maintained by their issuing bank where the User is then prompted to enter their authorization information, generally a password. Note that if the User has forgotten their authentication information, they may at this point contact their Issuer and begin a retrieval process via a link on the authentication page. Examples of the authorization pages can be found in the Appendix.

Depending upon the result of the verification, performed by the Issuer, the User will then either be directed back to an error page, or the Payment will proceed to the Acquirer for final approval.

Note that successful authentication of a registered card is not a sufficient condition for a Payment to be approved. In order for a Payment request to proceed to the 3-D Secure™ check, it must already have passed all checks configured by CQR and the Merchant, as well as be approved by the Acquirer as a final step. Conversely, if a card is not registered, the Payment is not necessarily rejected; the 3-D Secure™ check is simply not applied.

3 Benefits

3-D Secure™ authorization reduces the likelihood of chargeback incidents occurring with registered cards in two ways:

1. It is now much more difficult to use a stolen credit card, as Payments cannot be completed without entry of the owner's identifier.
2. Merchants may contest transaction disputes more effectively as it can be demonstrated that the disputed Payment was authorized by the owner.

In addition, Merchants have the opportunity to advertise the security and reliability of their online payment solution, in turn attracting the business of those Users who may be reluctant to submit credit card data online. The safety of online purchases made with the Merchant is demonstrated to users by the presence of the 3-D Secure™ authentication page. As the authentication page of both card networks is branded by the User's card issuing bank, User confidence in initiating the transaction is reinforced by brand familiarity.

Finally, as all communication with the card networks is undertaken by CQR, Merchant partners of CQR have little to no requirement (depending upon the chosen integration method with CQR) to change their existing card processing procedure in order to take advantage of this added layer of transaction security.

4 Further Reading

Both Visa and MasterCard provide information on 3-D Secure™ implementation and benefits on their respective websites.

Visa:

<https://partnernetwork.visa.com/vpn/global/category.do?userRegion=1&categoryId=85&documentId=117>

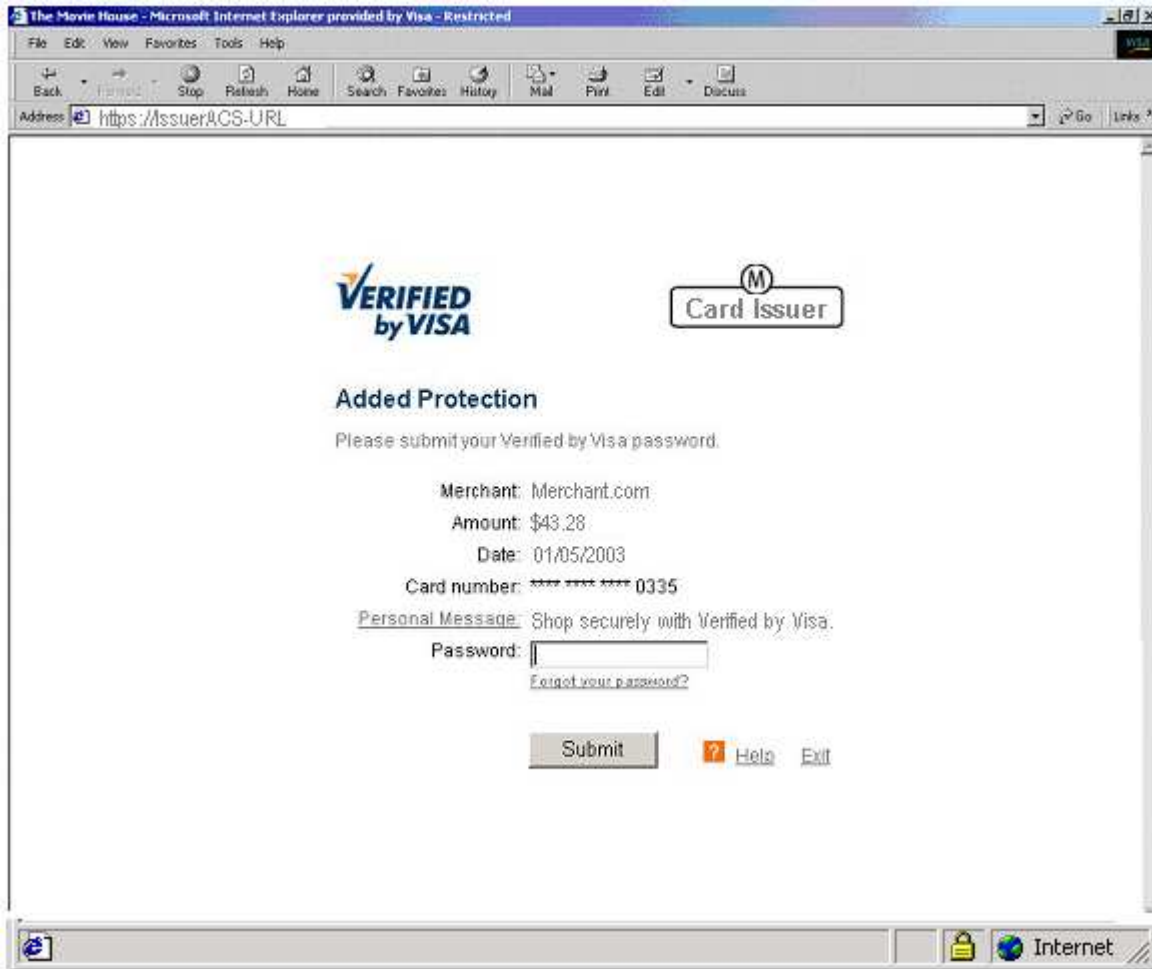
MasterCard:

http://www.mastercard.com/us/merchant/security/what_can_do/SecureCode/getting_started.html

Last Accessed: July 15th, 2009.

Appendix 1: Sample Authorization Pages

4.1 Verified by Visa



4.2 MasterCard SecureCode

