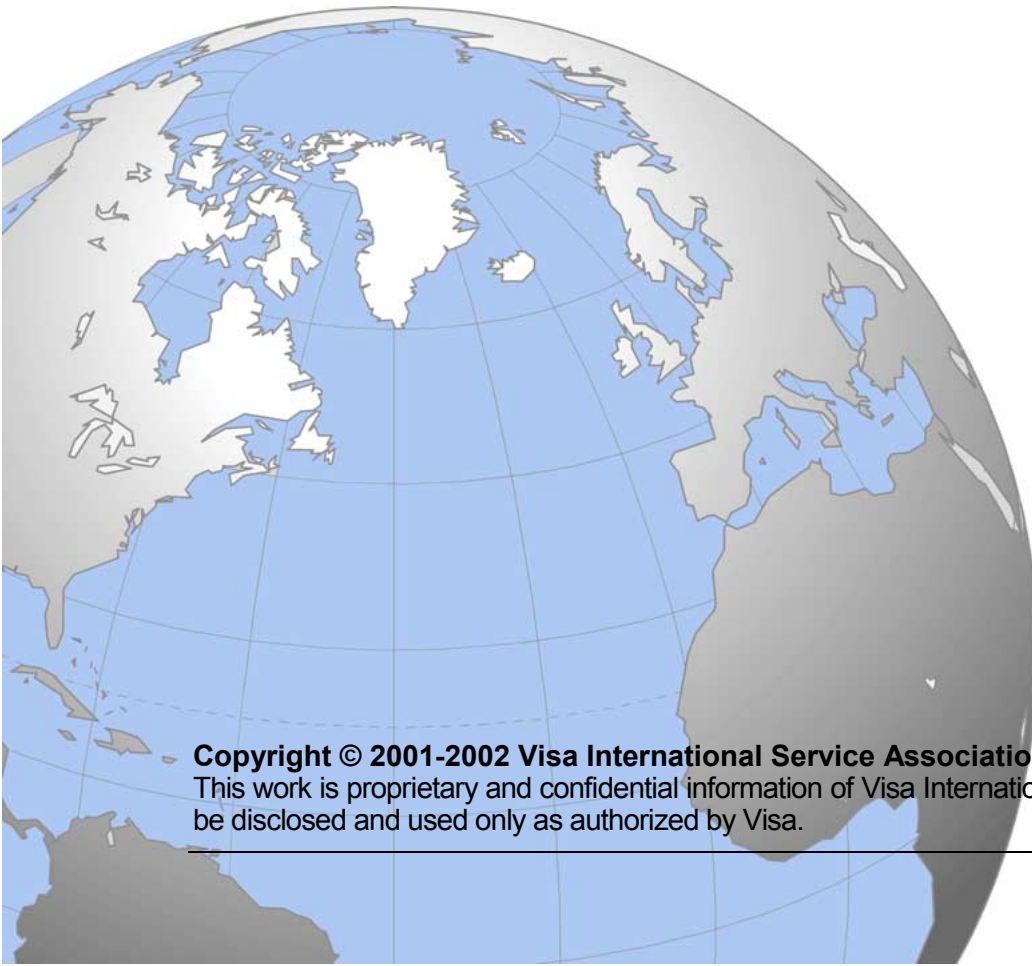




3-D Secure™

Introduction



Version 1.0.2
September 26, 2002

Copyright © 2001-2002 Visa International Service Association

This work is proprietary and confidential information of Visa International Service Association and may be disclosed and used only as authorized by Visa.

70001-01

Contents

1. Introduction.....	1
1.1 What is Payment Authentication?	1
1.2 Features	2
1.3 Benefits for Members.....	2
1.4 Options for Authenticated Payment	3
2. Benefits of 3-D Secure.....	5
2.1 System Benefits	5
2.2 Benefits for Acquirer	5
2.3 Benefits for Issuer	6
2.4 Benefits for Cardholder	6
2.5 Benefits for Merchants	6
3. Overview of 3-D Secure	7
4. How Does 3-D Secure Work?	9
4.1 Enrollment	9
4.2 Authentication	10
4.3 Merchant Perspective	12
4.4 Acquirer Perspective	12
4.5 Cardholder Perspective	13
4.6 Issuer Perspective	13
5. Member Considerations/Getting Started.....	15
5.1 Notify Visa Representative.....	15
5.2 Implementation Planning	15

Table of Figures

Figure 1: The Three Domains	7
Figure 2: Enrollment in 3-D Secure	9
Figure 3: Purchase Transaction Authentication	11

1. Introduction

The Internet and new access devices have created new online shopping convenience for Visa cardholders and merchants. Electronic commerce purchase volume continues to grow, and e-commerce transactions through VisaNet are expected to reflect that growth. As a relatively new shopping environment, the potential growth over the next five to ten years is significant. Even with these favorable trends, there are concerns regarding the potential for fraudulent use of payment cards on the Internet.

To address the added risk, Visa has implemented the Secure e-Commerce Initiative. This initiative is focused on increasing e-commerce transactions, promoting consumer confidence, and increasing Member and merchant profitability. The initiative includes three programs:

- Visa Account Information Security
- Visa Authenticated Payment
- Best Business Practices

This document provides a high-level introduction to 3-Domain Secure (3-D Secure™), a key component of the Visa Authenticated Payment Program. It is recommended that all Members, merchants, and solution providers involved in 3-D Secure implementation read this document before reading any of the other documents in the publication suite.

This document has been updated for 3-D Secure protocol version 1.0.2, and with the exception of Attempts processing, the information in this document also applies to version 1.0.1.

For more information regarding the other two programs of the Secure e-Commerce Initiative, please contact your Visa representative.

1.1 What is Payment Authentication?

As of July 2001, chargeback rates for Internet purchase transactions are several times the system average, and Internet-related fraud cases constitute a significant percentage of all reported fraud cases. The majority of the chargeback reasons are fraud-related or cardholders claiming non-participation.

To reduce the number of disputed online purchases, there is a need for a means to enable Issuers to verify that the person making an e-commerce purchase is an

authorized cardholder. This verification process is called “payment authentication.”

Visa has developed payment authentication capabilities to improve transaction performance online as well as to accelerate the growth of electronic commerce through increased consumer confidence. The objective is to provide Issuers with the ability to authenticate cardholders during an online purchase, in order to:

- reduce the likelihood of fraudulent usage of Visa cards, and
- improve transaction performance to benefit all participants.

The Visa Authenticated Payment Program ensures cardholder control over card use for online purchases, and provides payment security that adds an extra level of protection for both consumers and merchants.

1.2 Features

Payment authentication enables all parties in an e-commerce payment transaction to transmit confidential and correct payment data, and provides authentication that the buyer is an authorized user of a particular account. The Visa Authenticated Payment Program is a global program which supports potentially all Visa card products linked to an account with an Issuer (for example, it does not include Visa Cash cards). It also supports a variety of Internet access devices including, but not limited to:

- Personal computers
- Mobile phones
- Personal Digital Assistants (PDAs)

1.3 Benefits for Members

The primary benefit of 3-D Secure for Members is the reduction in disputed transactions and the resultant exception handling expense and losses. It is expected that nearly 80% of all e-commerce chargebacks and fraud, and a substantial proportion of customer complaints, could be eliminated with the use of Authenticated Payment. This will have a positive impact on Member profitability.

A less tangible, but nevertheless real, benefit is the assurance Members can provide to their cardholders who are considering e-commerce transactions. Studies indicate that as many as a third of cardholders are afraid to shop online due to security concerns. Authenticated Payment may convince prospective e-commerce shoppers that it is safe to use their card online.

Another benefit of 3-D Secure is the potential to leverage the infrastructure to support other financial and non-financial applications.

1.4 Options for Authenticated Payment

Although there are currently two protocols for Authenticated Payment, this document focuses on the approved global standard of 3-D Secure.

3-Domain Secure (3-D Secure) – Leverages Secure Sockets Layer (SSL) technology, which is incorporated in most browsers currently in use. This document highlights the features and benefits of this protocol.

SET Secure Electronic Transaction™ – This protocol uses cryptography to provide confidentiality of information, ensure payment integrity, and authenticate both merchants and cardholders.

More detailed information regarding SET™ is available at www.setco.org.

2. Benefits of 3-D Secure

2.1 System Benefits

The combined effect of ease and flexibility of implementation, secure transmission of account information, and reduced disputes offers the following benefits for all parties involved:

- Increased consumer confidence, leading to increased sales
- Increased card acceptance through better merchant confidence in accepting international transactions
- Reduced cardholder disputes, exception handling, retrievals, chargebacks, re-presentments, write-offs, and associated handling costs
- Increased likelihood of critical mass market adoption. 3-D Secure is a global service and is based upon the almost universal platform of Secure Sockets Layer (SSL)
- The ability to incorporate Visa Smart Debit Credit (VSDC) or equivalent chip cards. This 3-D Secure option provides the added assurance that the physical card is present during a transaction

2.2 Benefits for Acquirer

- Improved value to merchant by reducing the number of fraudulent user chargebacks, which represent the highest proportion of chargebacks in the Internet environment
- Improved value to merchants by providing the opportunity to increase sales and decrease disputed transactions

2.3 Benefits for Issuer

- Adds significant value to existing product offerings by enabling the authentication of Internet transactions, thus reducing the proportion of fraudulent transactions
- Increases Member online brand visibility because the Issuer is involved in each transaction, adding value and thus strengthening the Issuer relationship with the cardholder
- Provides Issuers with the opportunity to leverage existing cardholder authentication techniques such as those used for their online banking services
- No special application software is required on the cardholder's access device (except for chip card use)

2.4 Benefits for Cardholder

- Increased consumer confidence when purchasing on the Internet
- No special application software is needed at the cardholder access device (unless cardholder uses chip card)
- Easy to use
- Control over card use for online purchases

2.5 Benefits for Merchants

- Ease of integration into merchant legacy systems – only a software Plug-in and passing of data to VisaNet is required at the merchant/processor
- Minimal impact on merchant's interaction with consumer
- Increased sales by enhancing consumer confidence in online purchasing
- Reduced risk of fraudulent transactions
- Decrease in disputed transactions

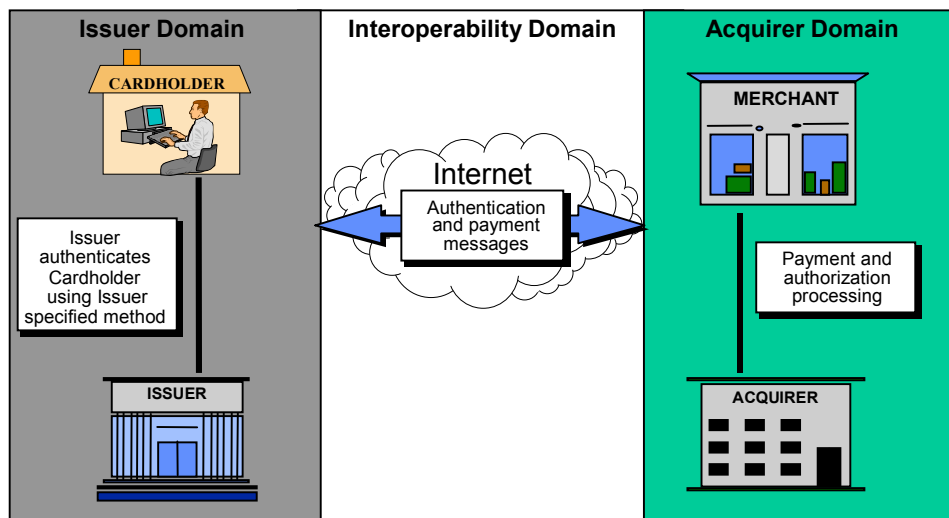
3. Overview of 3-D Secure

The 3-D Secure protocol underlies a new Visa payment service designed to enhance and validate payments made through the Internet. 3-D Secure is an authentication technology that uses Secure Sockets Layer (SSL) encryption and a Merchant Server Plug-in to:

- pass information and query participants to authenticate the cardholder during an online purchase, and
- protect payment card information as it is transmitted via the Internet.

3-D Secure is based on the three-domain model illustrated in Figure 1.

Figure 1: The Three Domains



Issuer Domain

The Issuer is responsible for:

- managing the enrollment of their cardholders in the service (including verifying the identity of each cardholder who enrolls) and authenticating cardholders during online purchases.

Acquirer Domain

The Acquirer is responsible for:

- defining the procedures to ensure that merchants participating in Internet transactions are operating under a merchant agreement with the Acquirer, and
- providing the transaction processing for authenticated transactions.

Interoperability Domain

This domain facilitates the transaction exchange between the other two domains with a common protocol and shared services.

4. How Does 3-D Secure Work?

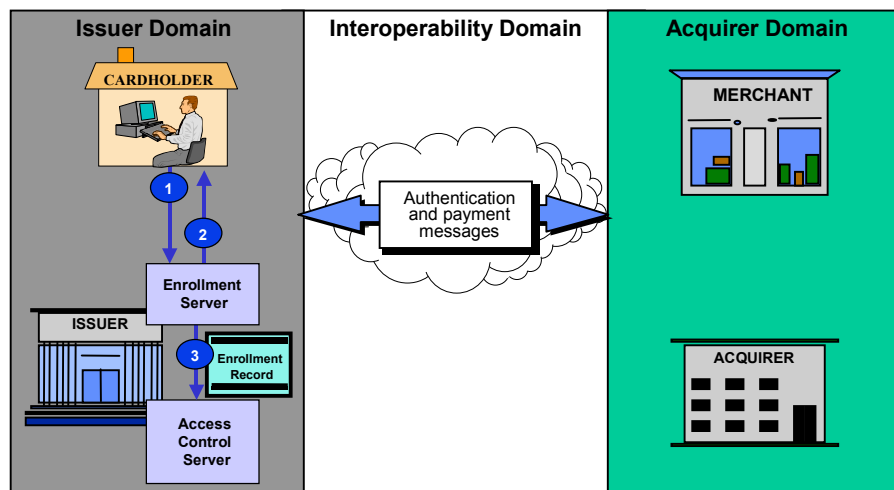
3-D Secure is comprised of two main functions: enrollment and authentication.

4.1 Enrollment

Enrollment is the process by which cardholders are enabled to use the service. When cardholders enroll, they are asked for relevant identification information as well as personal information such as a password and a Personal Assurance Message. (These will be used later at the time of purchase.) Once this data is collected and the Issuer has verified the cardholder responses, the cardholder is enrolled in 3-D Secure.

The Issuer's Enrollment Server tracks participating cardholders and passes the record of enrollment to the Issuer's Access Control Server. Each time the cardholder conducts a transaction for which a 3-D Secure authentication request is generated, this Access Control Server will be consulted to verify that the cardholder is in fact enrolled in 3-D Secure.

Figure 2: Enrollment in 3-D Secure



A sample enrollment procedure is as follows:

1. Cardholder goes to Issuer enrollment Web page and provides card number, expiration date, other identification information specified by the Issuer, and any required shared secret, such as a password or Personal Assurance Message.
2. Issuer validates cardholder-supplied information and notifies the cardholder of successful completion of the enrollment process.
3. The Enrollment Server supplies an update to the Access Control Server, including the newly enrolled card number and any other data required for subsequent purchase authentication, such as a password.

4.2 Authentication

After enrollment, the cardholder is ready to shop at any participating merchant site where the merchant has integrated the 3-D Secure Merchant Server Plug-in. The Merchant Server Plug-in is:

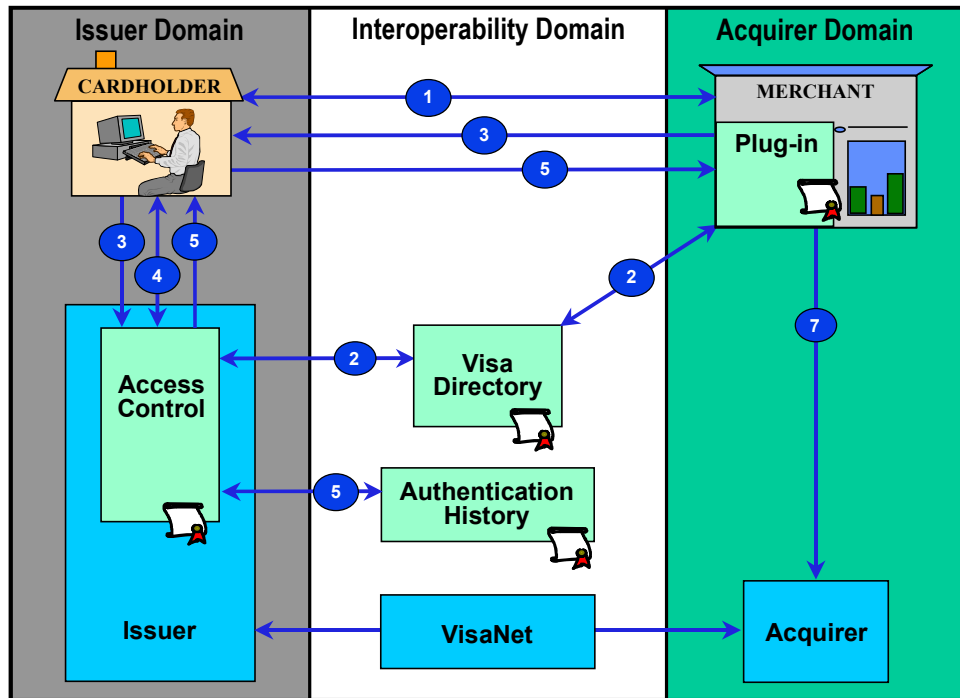
- integrated into a merchant's existing commerce server,
- able to obtain the cardholder information, and
- able to access the Issuer's Access Control Server to validate the card's participation in the service.

After the cardholder clicks "Buy", the Merchant Server Plug-in sends a message to the Visa Directory containing the cardholder account number. Through an exchange of messages, the Visa Directory and the Access Control Server determine if the cardholder is enrolled in 3-D Secure or if proof of attempted authentication is available. A message is returned to the Merchant Server Plug-in indicating the result. If the cardholder is enrolled or if proof of authentication attempt is available, the response includes the URL of the appropriate Access Control Server.

The Merchant Server Plug-in then sends an authentication request to the Access Control Server through the cardholder's browser. The Access Control Server performs the authentication routine defined by the Issuer. It may, for example, display a Personal Assurance Message to the cardholder and require that the cardholder respond with a password. The Access Control Server sends the results of the authentication to the Merchant Server Plug-in.

If the response message from the Access Control Server indicates successful cardholder authentication or proof of attempted authentication has taken place, the Merchant Server Plug-in returns the authentication response to the merchant and the transaction is processed as usual.

Figure 3: Purchase Transaction Authentication



A sample authentication procedure is as follows:

1. The cardholder selects goods or services and proceeds to the merchant's checkout page.
2. The Merchant Server Plug-in queries the Visa Directory to determine whether authentication or proof of attempted authentication is available for the card number. If the card number is in a participating card range, the Visa Directory queries the appropriate Issuer Access Control Server to validate cardholder participation or availability of proof of attempted authentication and sends the response back to the Merchant Server Plug-in.
3. The Merchant Server Plug-in sends an authentication request to the Access Control Server via the cardholder browser.
4. The Access Control Server queries the cardholder for password. The cardholder enters the password, and the Access Control Server verifies it.
5. The Access Control Server returns the authentication response to the Merchant Server Plug-in via the cardholder browser and passes a record of the authentication to the Authentication History Server.
6. The Merchant Server Plug-in validates the response.
7. If appropriate, merchant proceeds with authorization exchange with its acquirer.

4.3 Merchant Perspective

To participate in 3-D Secure, the merchant must integrate a Merchant Server Plug-in with their existing server. There are no changes to the customer-facing portion of the commerce application.

The Merchant Server Plug-in will generate messages to the Visa Directory and to various Access Control Servers in order to determine whether each shopper is an authorized user of the payment card being used.

If the authentication is successful, the merchant will process the authorization as usual, passing on authentication data to its acquirer, or acquirer's agent, for processing into VisaNet.

4.4 Acquirer Perspective

The Acquirer is responsible for contracting with merchants to offer the 3-D Secure service. Acquirers may assist merchants with the selection of a software technology vendor, and may provide implementation support as well as requirements for payment processing. Some Acquirers may also elect to provide e-commerce processing support, including 3-D Secure services, that are used by multiple merchants.

The Acquirer also assigns and manages merchant IDs, passwords, or certificates needed to authenticate their merchants in the system.

4.5 Cardholder Perspective

Most cardholders will enroll in 3-D Secure through a Web site operated by their Issuer. The cardholder is typically asked questions (determined by the Issuer) to establish their identity.

Once the identity of the cardholder is verified, the cardholder will be asked to create a shared secret, such as a password, that will be used during subsequent purchases.

From the cardholder's perspective, a 3-D Secure transaction is not substantially different from an ordinary e-commerce transaction. The cardholder shops in the usual manner. At checkout, once the cardholder enters their payment card information and clicks 'Buy', the 3-D Secure process is started. Typically, the cardholder's browser displays a new page which asks for the cardholder's authentication password. Once the password is verified and confirmed, the purchase is complete.

No special application software is required on the cardholder's access device when using a magnetic stripe card. A cardholder who has a Visa Smart Debit/Credit (chip) card will require a chip card reader and software to operate the reader.

4.6 Issuer Perspective

The Issuer is responsible for enrolling cardholders into the system as well as authenticating cardholders during 3-D Secure purchase transactions. The information for enrolled cardholders is stored in the Issuer's Access Control Server. When an authentication request is forwarded to the Issuer, the Access Control Server is queried to verify that the cardholder is enrolled. If the cardholder is enrolled, the Access Control Server will determine which authentication method (such as cardholder's password, or password and chip data from cardholder's chip reader) should be used in the transaction. Subject to regional requirements, the Issuer may also be required, or may optionally elect, to provide proof of authentication attempt functionality.

The Access Control Server then sends the results of the authentication process to the Merchant Server Plug-in and to the Authentication History Server.

5. Member Considerations/Getting Started

5.1 Notify Visa Representative

To participate in offering 3-D Secure services to cardholders and/or merchants, Members begin by notifying their Visa representative and completing the service enrollment process for 3-D Secure.

This ensures that information regarding participating Member BINs may be loaded in the 3-D Secure Interoperability Domain components supported by Visa:

- Visa Directory Server
- Authentication History Server

5.2 Implementation Planning

There are a variety of documents available to assist Members in implementing 3-D Secure. It is recommended that you next read:

3-D Secure: System Overview, Visa Publication 70015-01

3-D Secure: System Overview includes a detailed list of all 3-D Secure documents.

Implementation guides have been developed to help Issuers, Acquirers, and merchants to identify the requirements to offer 3-D Secure services. Additionally, the key areas involved in an implementation plan are highlighted to provide assistance in the development of plan components, key milestones, and time lines. Your Visa representative can provide copies of the 3-D Secure Implementation Guides and other documents in the 3-D Secure publication suite.