Verified by Visa Introduction

Verified by Visa

Effective: 30 December 2006

Contents

About This Guide

Chapter 1 • Introduction

Chapter 2 • Benefits of Verified by Visa

Chapter 3 • About the 3-D Secure Protocol

Chapter 4 • How Does Verified by Visa Work?

Chapter 5 • Member Considerations/Getting Started

Figures

About This Guide

Audience

This document provides a high-level introduction to Visa’s authentication service, Verified by Visa (VbV), and the 3-Domain Secure (3-D Secure™) protocol. It is recommended that all Members, merchants, and solution providers involved in VbV implementations read this document before any of the other documents in the publication suite.

Organization

The 3-D Secure Introduction Guide is organized into the following chapters:

- Chapter 1, Introduction—provides an introduction to payment authentication and Visa’s authentication service, Verified by Visa.
- Chapter 2, Benefits of Verified by Visa—provides a list of the benefits for Issuers, Acquirers, Cardholders, and Merchants.
- Chapter 3, About the 3-D Secure Protocol— provides a high-level overview of the 3-D Secure protocol, the technology foundation that the Verified by Visa service is based upon.
- Chapter 4, How Does Verified by Visa Work?—provides an overview of how the Verified by Visa service works.
- Chapter 5, Member Considerations/Getting Started—provides a list of considerations for getting started with the service.

Introduction 1

Secure e-Commerce Using Payment Authentication

The Internet and new access devices have created unprecedented online shopping convenience and venues for Visa cardholders and merchants. Electronic commerce purchase volume continues to grow, and e-commerce transactions through VisaNet reflect that growth. However, as commerce on the Internet increases, so do concerns regarding the potential for fraudulent use of payment cards in this card-not-present environment.

To address the added risk, Visa offers a payment authentication service that is focused on increasing e-commerce transactions, promoting consumer confidence, and increasing Member and merchant profitability.

This document provides a high-level introduction to Visa's payment authentication service, Verified by Visa (VbV), and the 3-Domain Secure (3-D Secure™) protocol. It is recommended that all Members, merchants, and solution providers considering Verified by Visa read this document before any of the other documents in the publication suite.

For more information, please contact your Visa representative.

What is Payment Authentication?

Chargeback rates for Internet purchase transactions are several times higher than face-to-face (e.g., cardholder present) chargeback rates. The majority of the chargeback reasons are fraud-related or cardholders claiming non-participation. To reduce the number of disputed online purchases, Issuers need a means 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 to improve transaction performance to benefit all participants.

Verified by Visa 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.

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. VbV is a global program which supports Visa card products linked to an account with an Issuer. It also supports a variety of Internet access devices including, but not limited to:

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

Benefits for Members

The primary benefit of VbV for Members is the reduction in disputed transactions and the resultant exception handling expense and losses. 80% of all e-commerce chargebacks and fraud, as well as 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 Verified by Visa is the potential to leverage the 3-D Secure infrastructure to support other financial and non-financial applications.

Benefits of Verified by Visa 2

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
- Globally-supported service
- Utilizes Secure Sockets Layer (SSL/TLS) encryption
- The ability to incorporate Visa Smart Debit Credit (VSDC) or equivalent chip cards. This Issuer option provides the added assurance that the physical card is present during a transaction.

Benefits for Acquirer

The benefits for acquirers include:

- 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

Benefits for Issuer

The benefits for issuers include:

- 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)

Benefits for Cardholder

The benefits for cardholders include:

- 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

Benefits for Merchants

The benefits for merchants include:

- 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

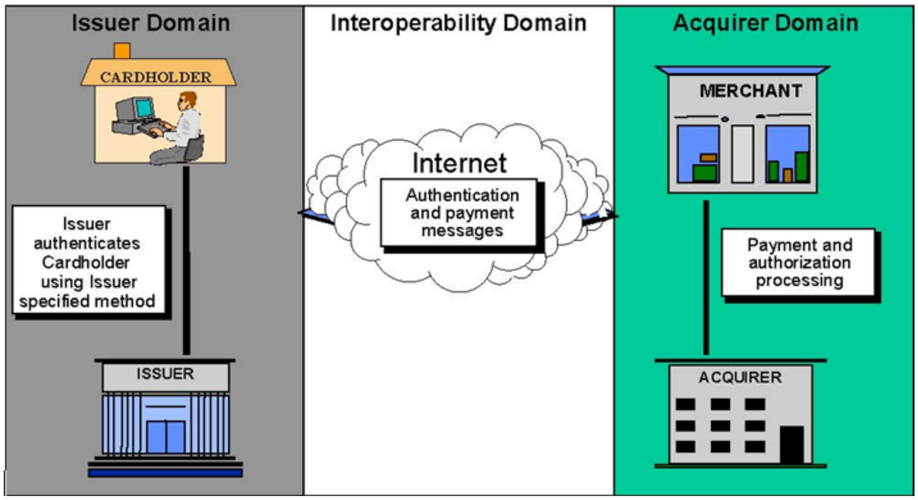
About the 3-D Secure Protocol 3

About the 3-D Secure Protocol

The 3-D Secure protocol underlies the Verified by Visa payment service. 3-D Secure is an authentication technology that uses Secure Sockets Layer (SSL/TLS) 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 3–1: The Three Domains


Issuer Domain
Interoperability Domain
Acquirer Domain
CARDHOLDER
MERCHANT
Internet
Authentication and payment messages
Issuer authenticates Cardholder using Issuer specified method
Payment and authorization processing
ISSUER
ACQUIRER

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.

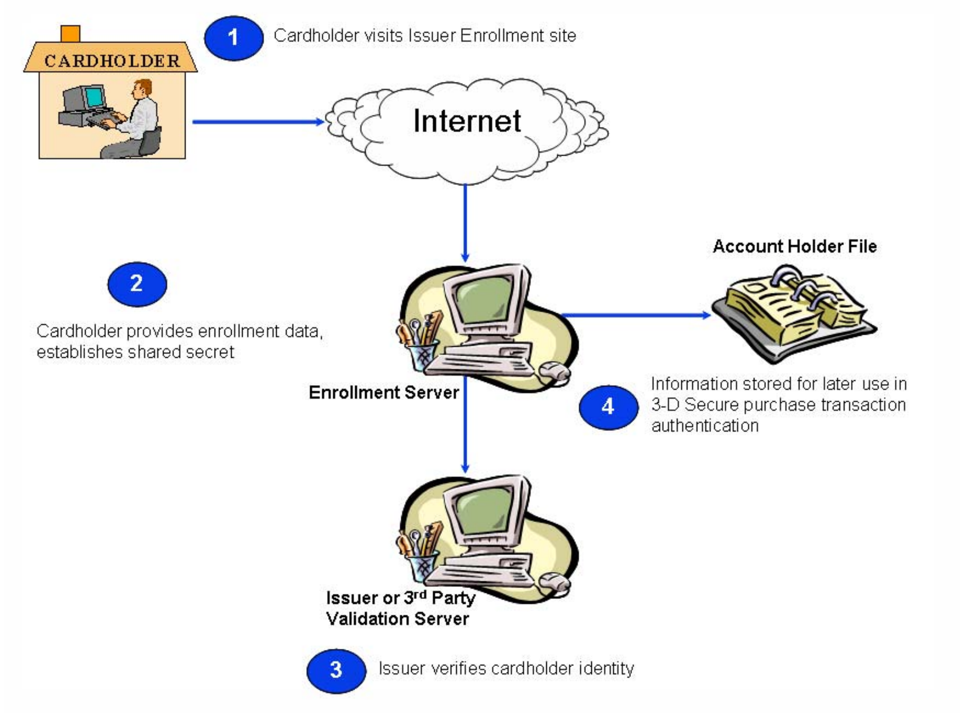
How Does Verified by Visa Work? 4

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 Verified by Visa.

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 Verified by Visa authentication request is generated, this Access Control Server will be consulted to verify that the cardholder is in fact enrolled in Verified by Visa.

Figure 4–1: Sample Cardholder Enrollment Process



CARDHOLDER
1
Cardholder visits Issuer Enrollment site
Internet
Account Holder File
2
Cardholder provides enrollment data, establishes shared secret
Enrollment Server
4
Information stored for later use in 3-D Secure purchase transaction authentication
Issuer or 3rd Party Validation Server
3
Issuer verifies cardholder identity

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.

Authentication

After enrollment, the cardholder is ready to shop at any participating merchant site where the merchant has integrated the Verified by Visa 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 an enrollment status request 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 Verified by Visa 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 (generally password but could be chip-car-based or other). For password entry, it displays a Personal Assurance Message to the cardholder and requires that the cardholder respond with a password. The Access Control Server verifies the password and 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 4–2 illustrates the authentication process.

Figure 4–2: Sample Purchase Transaction

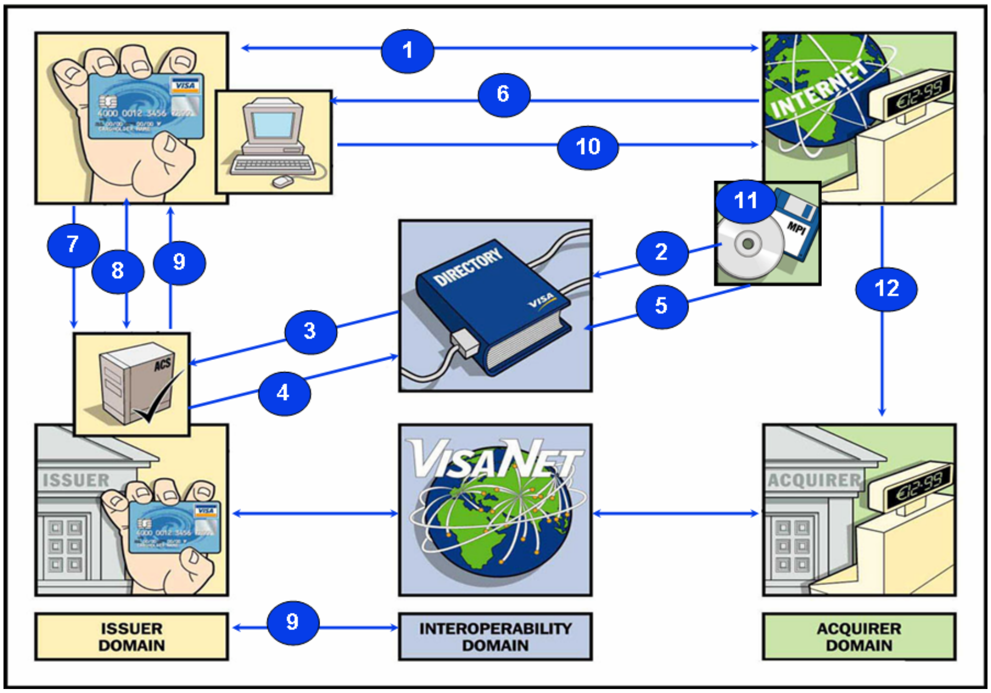


Table 4–1 lists the 12 steps of a purchase transaction, as illustrated in Figure 4–2.

Table 4–1: Sample Purchase Transaction (1 of 2)

Step 1	Shopper browses at merchant site, adds items to shopping cart, then finalizes purchase. Merchant now has all necessary data, including PAN and user device information.
Step 2	Merchant Server Plug-in (MPI) sends PAN (and user device information, if applicable) to Directory Server.
Step 3	Directory Server queries appropriate Access Control Server (ACS) to determine whether authentication (or proof of authentication attempt) is available for the PAN and device type. If no appropriate ACS is available, the Directory Server creates a response for the MPI and processing continues with Step 5.
Step 4	ACS responds to Directory Server.

Table 4–1: Sample Purchase Transaction (2 of 2)

Step 5	Directory Server forwards ACS response (or its own) to MPI. If neither authentication nor proof of authentication attempt is available, 3-D Secure processing ends, and the merchant, acquirer, or payment processor may submit a traditional authorization request, if appropriate.
Step 6	MPI sends Payer Authentication Request to ACS via shopper's device. The Payer Authentication Request message may be **PAReq** (for cardholders using PCs) or **CPRQ** (for cardholders using mobile Internet devices – see 3-D Secure: Protocol Specification – Extension for Mobile Internet Devices).
Step 7	ACS receives Payer Authentication Request.
Step 8	ACS authenticates shopper using processes applicable to PAN (password, chip, PIN, etc.). Alternatively, ACS may produce a proof of authentication attempt. ACS then formats Payer Authentication Response message with appropriate values and signs it. The Payer Authentication Response message is **PARes** if **PAReq** was received, or **CPRS** if **CPRQ** was received. (**CPRS** is created using values from the **PARes**.)
Step 9	ACS returns Payer Authentication Response to MPI via shopper's device. ACS sends selected data to Authentication History Server.
Step 10	MPI receives Payer Authentication Response.
Step 11	MPI validates Payer Authentication Response signature (either by performing the validation itself or by passing the message to a separate Validation Server).
Step 12	Merchant proceeds with authorization exchange with its acquirer. Following Step 12, acquirer processes authorization with issuer via an authorization system such as VisaNet, then returns the results to merchant.

Merchant Perspective

To participate in Verified by Visa, 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.

Acquirer Perspective

The Acquirer is responsible for contracting with merchants to offer the Verified by Visa 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 Verified by Visa 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.

Cardholder Perspective

Most cardholders will enroll in Verified by Visa 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 Verified by Visa 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 Verified by Visa 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.

Issuer Perspective

The Issuer is responsible for enrolling cardholders into the system as well as authenticating cardholders during Verified by Visa 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.

Member Considerations/Getting Started 5

Notify Visa Representative

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

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

- Visa Directory Server
- Authentication History Server

Implementation Planning

There are a variety of documents available to assist Members in implementing Verified by Visa. It is recommended that you next read *Verified by Visa System Overview*.

Verified by Visa System Overview includes a detailed list of all Verified by Visa and 3-D Secure documents.

Implementation guides have been developed to help Issuers, Acquirers, and merchants to identify the requirements to offer Verified by Visa. 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 Verified by Visa Implementation Guides and other documents in the 3-D Secure publication suite