Verified by Visa
System Overview
External Version 1.0.2

Verified by Visa

Effective: 30 December 2006

Contents

Chapter 3 • Architecture

Chapter 4 • Security

Chapter 5 • Visa Services

Figures

Tables

About This Guide

Purpose

Payment authentication is the process of verifying cardholder account ownership during a purchase transaction in an online commerce environment.

Visa has developed the Three-Domain Secure (3-D Secure™) protocol to improve transaction performance online and to accelerate the growth of electronic commerce. The objective is to benefit all participants by providing issuers with the ability to authenticate cardholders during an online purchase, thus reducing the likelihood of fraudulent usage of Visa cards and improving transaction performance.

Intended Audience

This document is intended for the use of any party that requires an understanding of the Visa Authenticated Payment program and the 3-D Secure protocol. Readers who require additional technical or operational information should then continue with the appropriate specifications (as described in Chapter 2, 3-D Secure Publication Suite).

Readers who prefer a higher level description may wish to read:

- *Verified by Visa Introduction*, 70001-01

Protocol Version

This document has been updated for 3-D Secure protocol Version 1.0.2.

NOTE: *With the exception of attempts processing, the information in this document also applies to Version 1.0.1.*

Organization

This document includes the following:

- A description of the Visa Secure e-Commerce Initiative, including 3-D Secure.
- A description of the 3-D Secure publication suite, including a summary of each document.
- A description of the architecture, entities, functions, and messages, including high level process diagrams for enrollment and transaction processing.
- A description of major security requirements and solutions, and related topics such as transport and message security, cardholder and merchant authentication methodologies, and the compliance and approval process for 3-D Secure Enrollment and Access Control Servers.
- A description of the 3-D Secure services provided by Visa.
- A discussion of implementation considerations for cardholder, issuers, acquirers, and merchants.
- A glossary of terminology and acronyms used throughout the suite of documents.
- A revision log summarizes the changes in each version of the document. Not included in this document

Document Organization

This document is organized as follows:

Chapter 1—describes the Visa Secure e-Commerce Initiative, including 3-D Secure.

Chapter 2—describes each document in the 3-D Secure publication suite.

Chapter 3—describes the Three Domain Model within which 3-D Secure was designed and the entities that participate in 3-D Secure. It includes high-level message and control flow diagrams with step-by-step explanations of what happens during cardholder enrollment and during the authentication of a purchase transaction.

Chapter 4—describes the security requirements for 3-D Secure and the solutions selected to address them. It discusses how the confidentiality of messages is ensured, and how the cardholder and merchant are authenticated.

Chapter 5—briefly describes the Visa interoperability services and the optional Visa enabling services.

Chapter 6-9—describe at a high level a wide variety of implementation considerations and options for each of the primary participants – cardholder, issuer, acquirer, and merchant.

Glossary—defines terminology and acronyms used throughout the publication suite.

Document Conventions

The document conventions used in this guide are shown in Table 1.

Table 1: Document Conventions

Document Convention	Purpose In This Guide
`LetterGothic` typeface	Entries typed at the keyboard, messages displayed by the system, and the typeface used to re-create screen captures and sample report layouts in text.
To do	Indicates step-by-step procedures. For example: To obtain information about specific test data:
EXAMPLE	Identifies an example of what the accompanying text describes or explains.
IMPORTANT	Highlights important information in the text.
italics	Document titles; emphasis.
“text in quote marks”	Section names referenced in a chapter.
NOTE:	Provides more information about the preceding topic.

Visa Secure E-Commerce Initiative 1

Purpose

Programs

To leverage e-commerce opportunities, Visa has developed 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 the following programs:

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

The objectives of the Best Business Practices and Account Information Security Programs are to describe best practices and establish standards for e-commerce merchants to help them ensure that cardholder data is secure at their sites. The objective of the Authenticated Payment Program is to authenticate cardholders within the Three Domain Model (described in Chapter 3, Architecture, section “Three Domain Model” on page 3–2).

Visa Authenticated Payment

There are currently two protocols for Authenticated Payment:

- **3-D Secure™** – Leverages Transport Layer Security (TLS) technology, which is incorporated in most browsers currently in use. Provides confidentiality of information, ensures payment integrity, and authenticates cardholders.

  NOTE: *TLS is the successor to Secure Sockets Layer (SSL).*

- **SET Secure Electronic Transaction™** – Uses cryptography to provide confidentiality of information, ensure payment integrity, and authenticate both merchants and cardholders.

This document focuses on the approved global standard of 3-D Secure.

3-D Secure Protocol Features

Features of the 3-D secure protocol are:

- Provides global framework for the authentication of remote payments
- Reduces operational expense by minimizing chargebacks for unauthorized use
- Can be implemented without requiring specialized cardholder software or hardware
- Can be enhanced by the issuer as needed to meet customer management and security requirements without impact on the acquirer or merchant
- Is extensible into emerging channels such as mobile telephones, PDAs, and digital TV
- Is based on globally accepted technical standards provided by international standards bodies such as the Internet Engineering Task Force (IETF)
- Provides a centralized archive of payment authentications for use in dispute resolution

3-D Secure Publication Suite 2

Purpose

A full set of documentation has been developed for 3-D Secure. For convenience, these publications are divided into the following categories as listed in Table 2–1.

Table 2–1: Categories of 3-D Secure Documentation

Category	Description
Introductory Publications	Provides introductory information regarding 3-D Secure from a service and a system perspective.
Product Publications	Provides information to help developers design and build 3-D Secure products. They include both core specifications and specifications for value-added and optional features.
Services Publications	Provides service specifications on various components of 3-D Secure, such as the Visa Directory Server, Access Control Server, etc.
Implementation Publications	Provides 3-D Secure service implementation information for issuers, acquirers, merchants, and regions.
Compliance Publications	Provides the requirements that developers of 3-D Secure products must meet to establish that their products comply with the 3-D Secure specifications.

Licensed Documents

Some 3-D Secure documents are available only to parties that have executed with Visa a 3-D Secure Publication Suite Master License Agreement. Information regarding these publications and the license agreement is available through the *Vendors & Merchants* link at:

`http://corporate.visa.com.`

Introductory Publications

These documents provide an introduction to 3-D Secure at different levels of detail as listed in Table 2–2.

Table 2–2: 3-D Secure Introductory Publications

Purpose	Document Number	Description
Introduction	70001-01	Provides a high-level description of the Visa Secure e-Commerce Initiative, including 3-D Secure. Describes how 3-D Secure works; the benefits to members, merchants, and cardholders; and member considerations for adoption and implementation. All parties interested in 3-D Secure are encouraged to read this document first.
System Overview	70040-01	Provides an introduction and guide to the entire 3-D Secure service. All parties interested in 3-D Secure are encouraged to read this document after the **Introduction** and before any other 3-D Secure publications.

Product Publications

These documents provide information to help developers design and build 3-D Secure products and are listed in Table 2–3.

Table 2–3: 3-D Secure Product Publications

Purpose	Document Number	Description
Protocol Specification–Core Functions	70000-01 *Licensed*	Details of 3-D Secure setup, cardholder enrollment, protocol, and processing steps, along with detailed message formats; primarily focused on messages exchanged across the Interoperability Domain. ***Note:*** *The protocol specified in document 70000-01 is referred to throughout the publication suite as "the core protocol."*
Functional Requirements–Access Control Server	70002-01 *Licensed*	Describes functional requirements for Access Control Server (ACS) software, including configuration, enrollment, interaction with the Visa Directory Server, authentication message processing, message transmission to the Authentication History Server (AHS), transaction logging, internationalization, and data formats.
Functional Requirements–Merchant Server Plug-in	70003-01 *Licensed*	Describes functional requirements for Merchant Server Plug-in (MPI) software, including configuration, interaction with the Visa Directory Server, message processing, signature validation, transaction logging, formats, and implementation options.
Functional Specification–Chip Card Authentication	70005-01 *Licensed*	Identifies and describes the technical and security specifications of an authentication method for Visa Smart Debit/Credit cards.
Protocol Specification–Extension for Mobile Internet Devices	70006-01 *Licensed*	Discusses the implementation issues and specifies the protocol changes required for 3-D Secure to support Internet-capable mobile devices, such as WAP phones.
Protocol Specification–Extension for Voice and Messaging Channels	70004-01 *Licensed*	Describes the protocol changes required to support the use of SMS, USSD, or voice/IVR for shopping and authentication within the 3-D Secure protocol and related implementation issues.

Services Publications

The Services documents listed in Table 2–4 describe each of the main components of the 3-D Secure service and their required functions.

Table 2–4: 3-D Secure Services Publications

Purpose	Document Number	Description
Service Specification Visa Directory	70007-01	The Visa Directory Server component of the 3-D Secure service enables a merchant to confirm that a given cardholder is enrolled in 3-D Secure and to locate the appropriate Access Control Server (ACS) to allow the issuer to authenticate the cardholder for the current transaction. The Service Specification for the Visa Directory Server describes the functions of this component.
Service Specification Authentication History Service	70008-01	This document describes the Visa-operated Authentication History Service, which provides a central location (the Authentication History Server) where Access Control Servers store a record of the outcome of each payment authentication transaction and other information for dispute resolution and reporting purposes.
Enabling Service Specification Enrollment Service	70009-01	The Enrollment component of the 3-D Secure service provides a mechanism whereby the issuer can enroll their cardholders for participation in 3-D Secure. This document describes the required functions of the Enrollment component.
Enabling Service Specification Access Control Service	70010-01	The Access Control Server (ACS) component of the 3-D Secure service provides a mechanism whereby the issuer can provide authentication of their cardholders for each purchase transaction with a 3-D Secure enabled merchant. This document describes the required functions of the Access Control Server.

Implementation Publications

The Implementation publications listed in Table 2–5 provice information to members and regions to help them plan, implement, and operate successful 3-D Secure Authenticated Payment Programs.

Table 2–5: 3-D Secure Implementation Publications

Purpose	Document Number	Description
Service Activation Guide	70011-01	The Service Activation Guide provides information to help the region plan, implement, and operate a successful 3-D Secure Authenticated Payment Program.
Implementation Guide Issuer	70013-01	The Issuer Implementation Guide provides information to help the issuer plan, implement, and operate a successful 3-D Secure Authenticated Payment Program.
Implementation Guide Acquirer	70014-00	The Acquirer Implementation Guide provides information to help the acquirer plan, implement, and operate a successful 3-D Secure Authenticated Payment Program.
Implementation Guide Merchant	70020-01	The Merchant Implementation Guide provides information to help the merchant plan, implement, and operate a successful 3-D Secure Authenticated Payment Program.
Mobile Authentication Scenarios	70022-01	The Mobile Authentication Scenarios Guide provides information to help issuers determine the most appropriate cardholder authentication mechanisms to support their mobile implementations of 3-D Secure.

Compliance Publications

Developers of 3-D Secure products must establish that their products comply with 3-D Secure specifications by completing compliance testing. The documents listed in Table 2–6 describe the requirements for that testing and how the System Test Facility may be used in preparation for compliance testing.

In addition, developers of 3-D Secure issuer products, as well as those that host these products, must meet the requirements described in *3-D Secure Security Requirements – Enrollment and Access Control Servers*.

Table 2–6: 3-D Secure Compliance Publications

Purpose	Document Number	Description
Compliance Testing Facility–Policies and Procedures	70017-01	Describes the compliance and auditing program, including policies, procedures, facilities, fees, kind of products tested, and legal agreements.
Compliance Testing Facility–User Guide	70018-01	Supplies detailed information about using the compliance testing facility provided by Visa, including facility procedures, the test tools and how to use them, the kinds of tests that are performed, controls, and equipment configurations.
System Test Facility –Policies and Procedures	70021-01	Describes a testing environment intended for use by vendors of 3-D Secure software components and by Visa members, to functionally test a software component (Access Control Server or Merchant Server Plug-in) for *end to end* payment transaction execution.
Security Requirements–Enrollment and Access Control Servers	70016-01 *Licensed*	Describes Visa requirements and standards that must be met, and the process for approval and activation of a 3-D Secure Enrollment or Access Control Server.

Architecture 3

Purpose

This chapter describes the Three Domain Model within which the entities involved in 3-D Secure work together to authenticate and authorize an online payment transaction. The role of each entity is described and two simple transaction process diagrams show the messages that move among them.

Three Domain Model

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

- **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.

NOTE: *Third parties operate many of the systems in the Issuer and Acquirer Domains on behalf of Visa members in accordance with Visa non-member agent requirements.*

Figure 3–1 provides a simple illustration of the participants in their associated domains.

The Three Domain Model enables issuers to authenticate their cardholders during online purchases. Acquirers and merchants have a flexible framework that can embrace a variety of technical approaches. Interoperability between the issuer and acquirer is achieved through the use of a common protocol and the Visa interoperability services described in Chapter 5, Visa Services.

Figure 3–1: The Three Domain Model

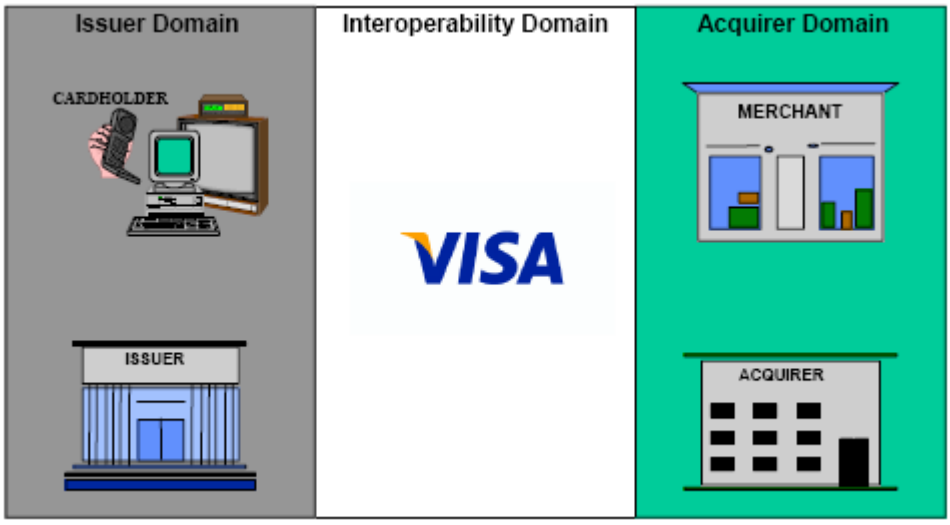
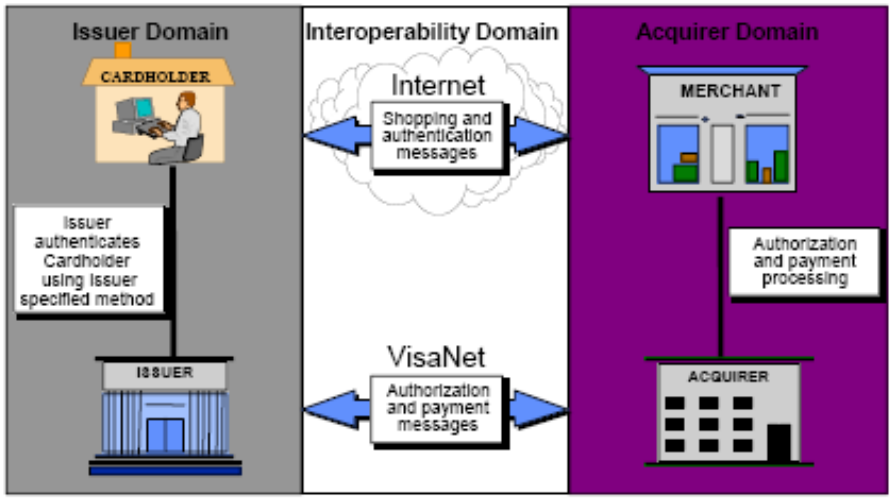


Figure 3–2 illustrates the basic functions of 3-D Secure.

- 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.

Figure 3–2: 3-D Secure Within the Three Domain Model



3-D Secure Entities

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

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 that authenticate cardholders using passwords should not require any additional 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 the 3-D Secure service
- Defines card number ranges eligible to participate in the 3-D Secure service
- Provides data about those card number ranges to the Visa Directory Server
- Performs enrollment of the cardholder for each payment card account (via the Access Control Server, a separate Enrollment Server, or manually)

Access Control Server—The Access Control Server (ACS) has two functions:

1. To verify whether 3-D Secure authentication (or proof of attempted authentication) is available for a particular card number
2. To authenticate the cardholder for a specific transaction or to provide proof of attempted authentication when authentication is not available

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

Merchant—Existing merchant software handles the shopping experience, obtains the card number, and then invokes the Merchant Server Plug-in to conduct payment authentication.

After payment authentication, the merchant software may submit an authorization request to the acquirer, if appropriate.

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, a separate server, the acquirer, or a third party may perform this function.

Acquirer—A Visa member financial institution that:

- Enters into a contractual relationship with a merchant for purposes of accepting Visa cards
- Determines the merchant's eligibility to participate in the 3-D Secure service

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

Visa Directory Server—The Visa Directory Server, operated by Visa:

- Receives messages from merchants 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 (which may or may not provide attempts functionality) or responds directly to the merchant
- Receives the response from the ACS indicating whether payment authentication (or proof of attempted authentication) is available for the cardholder account
- Forwards the response to the merchant

Commercial Certificate Authority—Generates selected certificates for the use of 3-D Secure entities, including:

- SSL/TLS client and server certificates

Visa 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

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

Section, "Purchase Transaction Flow," provides more detail about messages and control flows.

Cardholder Purchase—When checking out at the conclusion of shopping, the 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 may be located at the merchant shopping site, at the acquirer, or at a third-party processor site.

Request to Visa Directory Server—The MPI sends a message to the Visa 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 or if proof of authentication attempt is available, the response message instructs the MPI on how to contact the Access Control Server (ACS) of the associated issuer.
- If the account number of the cardholder falls outside of participating card ranges, the Visa Directory Server returns the transaction to the merchant's commerce server via the MPI and the merchant proceeds with a standard authorization request.

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 a password, or by some other authentication method, such as a Visa chip card.

The ACS formats and digitally signs the authentication response, then returns it to the MPI.

Payment Processing—If the authentication response indicates successful authentication or proof of authentication attempt, the merchant forwards an authorization request with the requisite data to its acquirer or the acquirer's processor for submission into VisaNet.

Purchase Transaction Flow

Figure 3–3 illustrates the basic message flows in the case of a cardholder accessing the merchant through a PC using the Internet. The steps listed in Table 3–1 describe the processing indicated by the numbered arrows in Figure 3–3.

Figure 3–3: Purchase Transaction Flow

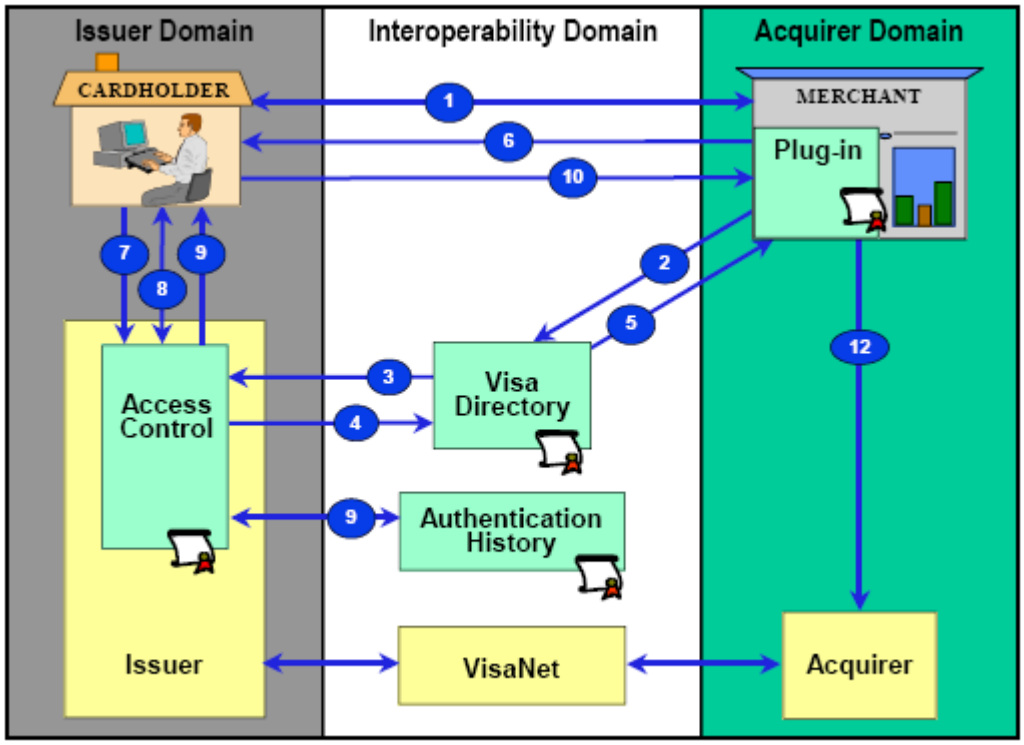


Table 3–1: Purchase Transaction Flow

Step 1	Shopper browses at a merchant site, selects items, and then finalizes the purchase. ***Note:*** *The merchant now has all the necessary data, including card number and user device information.*
Step 2	The Merchant Server Plug-in (MPI) sends the PAN (and user device information, if applicable) to the Visa Directory Server.
Step 3	The Visa Directory Server queries the appropriate Access Control Server (ACS) to determine whether authentication (or proof of attempted authentication) is available for the PAN and device type. ***Note:*** *If an appropriate ACS is not available, the Visa Directory Server creates a response for the MPI and processing continues with Step 5.*
Step 4	The ACS responds to the Visa Directory, indicating whether authentication (or proof of attempted authentication) is available for the card number.
Step 5	The Visa Directory Server forwards the ACS response (or its own) to the MPI. If neither authentication nor proof of attempted authentication is available, the merchant, acquirer, or payment processor submits a traditional authorization request.
Step 6	The MPI sends a Payer Authentication Request **(PAReq)** to the ACS via the shopper's device.
Step 7	The ACS receives the **PAReq**.
Step 8	The ACS either authenticates the shopper by using processes applicable to the card number (password, chip, PIN, etc.) or if attempts ACS functionality is available, creates the proof of authentication attempt. The ACS then formats the **PARes** message with the appropriate values and signs it.
Step 9	The ACS returns the **PARes** to the MPI via the shopper's device. The ACS sends selected data to the Authentication History Server (AHS).
Step 10	The MPI receives the **PARes**.
Step 11	The MPI validates the **PARes** signature (either by performing the validation itself or by passing the message to a separate Validation Server).

Table 3–1: Purchase Transaction Flow (continued)

Step 12	If appropriate, the merchant proceeds with the authorization exchange with its acquirer. Following Step 12, the acquirer processes the authorization request and returns the authorization response to the merchant.

Sample Enrollment Procedure

Figure 3–4 illustrates a possible enrollment process.

This is only a sample. Since the cardholder enrollment process is entirely within the Issuer Domain, alternative implementations are likely.

The steps listed in Table 3–2 refer to the processes indicated by the numbers in Figure 3–4.

Figure 3–4: Sample Cardholder Enrollment Process

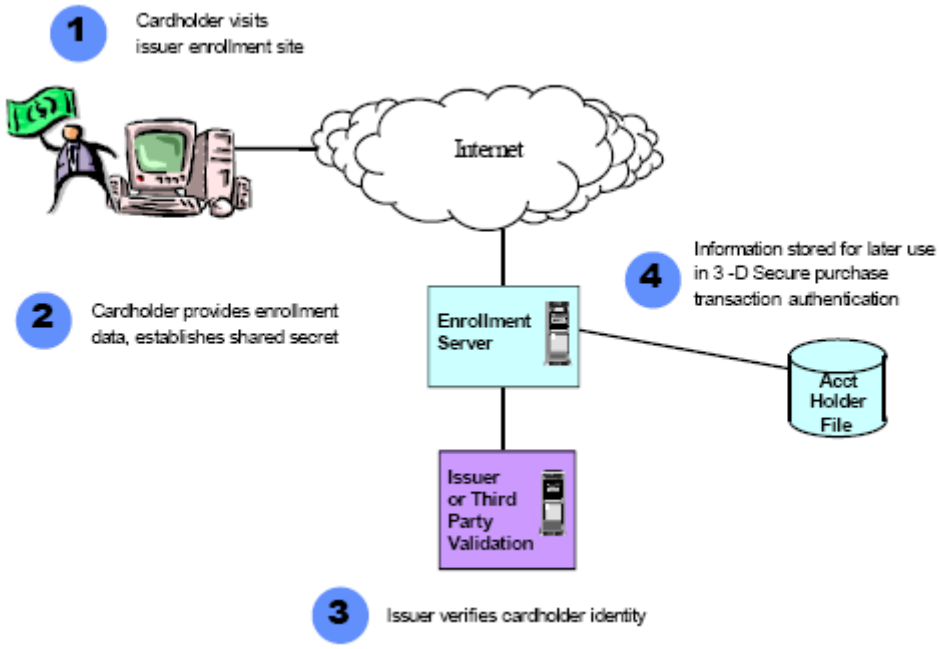


Table 3–2: Sample Cardholder Enrollment Process

Step 1	The cardholder visits the issuer's 3-D Secure Enrollment Web page.
Step 2	The cardholder supplies payment card number and provides other enrollment information with the Enrollment Server that will enable the issuer to validate cardholder identity, and establish any required shared secret, such as a password.
Step 3	The issuer or third party validates the information provided in Step 2 to verify that the cardholder is entitled to use the payment card being enrolled. In the case of a Visa smart card, the verification process also establishes that the cardholder has physical possession of the card at the time of enrollment.
Step 4	Information is stored for validation during authentication processing. The cardholder is informed of success (or failure) of enrollment. The cardholder is ready to go shopping as soon as enrollment is confirmed.

Security 4

Purpose

This chapter discusses the primary security requirements that were established for 3-D Secure, and the solutions selected to satisfy those requirements. The chapter also describes the security requirements that must be met for an entity to receive approval to activate and operate a 3-D Secure Enrollment or Access Control Server.

Security Requirements and Solutions

The Visa Authenticated Payment Program, including 3-D Secure, was developed to address the following key security requirements:

- Confirm cardholder identity prior to authentication processing.

  Solution: Cardholder identity verification during enrollment using issuer-defined validation process

- Enable secure and reliable communication channels between cardholder and issuer using a server certificate and the strongest cryptography the cardholder browser supports.

  Solution: SSL/TLS

- For each purchase, ensure that the person presenting a payment card is entitled to use that card.

  Solution: Successful authentication dialog between cardholder and issuer

- Establish authenticated, secure communication channels among all non-cardholder entities using cryptographically strong facilities.

  Solution: SSL/TLS sessions established only with known parties who are authenticated using certificates or who log on using Visa-managed ID and password

- Provide confidentiality of payment and order information by using underlying transport-level strong cryptographic facilities.

  Solution: SSL/TLS

- Ensure integrity of authentication response and confirmation that the response originated from the card issuer.

  Solution: Visa-enabled strong issuer digital signature on authentication response

- Encourage, and require where possible, the best commercial security practices and technology to protect the interests of all parties to the trust model. These include specific protocols, requirements, guidelines, and compliance tests as described in the documents comprising the 3-D Secure publication suite, the Visa Account Information Security Program, Visa International and Regional Operating Regulations, and other related Visa publications.

Transport and Message Security

Transport Security

Some 3-D Secure messages have built-in provisions for security that are independent of the transport technology. Others depend upon security techniques provided by the transporting facilities. All depend upon transport security to provide confidentiality. As a consequence, transport security is always required.

Message Security

Messages in 3-D Secure flow among entities both within and between the three domains. Various fundamental technologies are used to protect the confidentiality of those messages, and to ensure the authenticity of the parties sending and receiving the messages. The technologies that are used include:

- ID and password
- Public key cryptography, including digital certificates
- Hardware security modules
- Practices and procedures prescribed by published Visa policies and guidelines
- Digital signatures (used to ensure that the authentication response from the issuer Access Control Server is valid)
- Transport level security

Cardholder Authentication

Issuer Chooses Authentication Method

The publication suite describes cardholder authentication by means of a password or personal identification number, possibly accompanied by a cryptogram generated by a chip card. Details are provided in the following documents:

- *3-D Secure: Protocol Specification – Core Functions, Visa Publication 70000-01 (licensed)*
- *3-D Secure: Functional Specification – Chip Card Authentication, Visa Publication 70005-01 (licensed)*

While the 3-D Secure model facilitates the use by issuers of other authentication technologies, Visa regions may establish rules that require members to review their proposed authentication technologies with their Visa region. Additional technologies may be reviewed by Visa for particular purposes, such as support for mobile devices. Issuers should consult their Visa representatives for details.

Implementation of Defined Methods

During enrollment, issuers use whatever means they choose to verify that the enrolling party is entitled to use the payment card presented.

When passwords are used (as described in the core protocol), the cardholder is asked to choose a password during enrollment. During each subsequent authentication request, the issuer, via the Access Control Server, ensures that the password provided by the shopper matches the one established during enrollment.

When chip cards are used, the enrollment process can be enhanced by authenticating the card using a cryptogram to ensure that a Visa smart card for the account being enrolled is in the possession of the cardholder at the time of enrollment. Additional options for chip cards include validating that the cardholder is able to successfully perform offline PIN verification, where supported by the issuer.

Merchant Authentication

Merchant authentication is the process of identifying a specific merchant and determining whether the merchant is authorized to participate in 3-D Secure.

The merchant is authenticated on each 3-D Secure transaction passing from the Merchant Server Plug-in to the Visa Directory Server.

Authentication Methods

Depending on the requirements of each Visa region, merchant authentication may be implemented using either certificates or merchant ID and password.

Acquirers should consult with their Visa representatives regarding merchant authentication methods for their Visa region.

Server Activation

Server Approval and Activation

Both Visa members and non-members may be approved to offer Enrollment and Access Control services. Before those services can be activated or the hosting begin, the entity must meet certain requirements, complete the process outlined in section, "*Approval and Activation Process*," and be approved for activation by Visa. For information about the requirements and approval process, see:

- *3-D Secure: Security Requirements – Enrollment and Access Control Servers, Visa Publication 70016-01 (licensed)*

These requirements identify issues that must be addressed in the design and operations of the system. The issuer and the service provider are responsible for providing documentation that describes their approach to the system design and operation, and the methods and results of any procedures or reviews that are undertaken to ensure that the requirements have been met.

Approval and Activation Process

The following list presents highlights of the approval and activation process.

- Pass a field review. This review is not required for members that provide services solely to their own base of cardholders; however, they may request this review. In addition, at its discretion, Visa may review such members. There is an inspection fee for conducting a field review.
- Complete the 3-D Secure Enrollment/Access Control Server Security Standards Self-Audit. A copy is available in the *3-D Secure Security Requirements – Enrollment and Access Control Servers, Visa Publication 70016-01 (licensed)*
- Members using a third-party service provider must register the service provider following the registration requirements as outlined in the Visa Operating Regulations.
- If a member, register for participation in 3-D Secure with the Visa region.
- Meet security standards for:
  - Key management and security of keys including generation, loading, usage, storage, backup, termination, archiving, and compromise.
  - Physical security such as providing certain access control systems, alarms, construction, locking devices, procedures, intrusion detection, and dual control over access to cryptographic materials.
  - System security controls such as protection from unauthorized access, modification, substitution, insertion, deletion including meeting the requirements for a Trusted Computing Base as described in the Orange Book (the U.S. Department of Defense *Trusted Computer System Evaluation Criteria*) or the Common Criteria Target of Evaluation Security Functions (see *Common Criteria for Information Technology Security Evaluation, Part 2*, Version 2.1 publication number CCIMB-99-032 and related documents available at:

    http://www.commoncriteria.org/cc/cc.html).
  - Written staff acceptance of responsibility and background checks.
  - Change control systems that include the ability to ensure that unauthorized or untested changes to production code do not occur, documentation for change processes, emergency change procedures, executable to source code matching, and segregation of duties.
  - Special requirements where multiple issuers are supported.
  - Firewalls and server protection from network-based threats.
  - Business resumption planning and testing.

Visa Services 5

Purpose

This chapter discusses services offered by Visa for implementing 3-D Secure. Chapters 6-8 discuss specific implementation considerations for various parties: cardholder, issuer, merchant, and acquirer.

Visa 3-D Secure Services

Visa provides two types of service for members and merchants implementing 3-D Secure:

Interoperability services provided exclusively by Visa International	Visa Directory Service Authentication History Service
Enabling services that may be provided by Visa regions, and that issuers may choose to use	Enrollment Service Access Control Service Proof of Attempt Service

These services provide a powerful, fully functional core of capabilities that enable rapid adoption of 3-D Secure by issuers, acquirers, and merchants.

Visa Directory Service

The Visa Directory Service provides the enabling interface that merchants use to determine whether cardholders are enrolled in 3-D Secure, and which ACS to contact for each payment authentication attempt.

Merchants query the Visa Directory Server to determine whether an account number is enrolled in 3-D Secure or whether proof of authentication attempt is available. The Visa Directory Server responds directly if the account number is not part of a participating range or proof of attempt is not available. Otherwise, it forwards the request to the appropriate Access Control Server, receives its response, and forwards the response to the merchant.

Authentication History Server

The Authentication History Server provides a common repository where issuers store copies of all authentication requests and results for dispute resolution and other purposes.

Optional Visa Enabling Services

To enable issuers to adopt and implement 3-D Secure, Visa regions may operate enabling services for two major 3-D Secure components: an Enrollment Server and an Access Control Server. In addition, Visa regions may provide attempts functionality as part of their enabling services offering to issuers. Members interested in additional information should ask their Visa representative.

Cardholder Implementation Considerations 6

Purpose

For the core services of 3-D Secure, cardholders only need to decide whether to enroll in the service offered by their issuers. If issuers offer value-added authentication technologies such as chip card, then the cardholder becomes more involved in the process and the issuer may need to provide special software or training to the cardholder.

Cardholders will be able to use 3-D Secure from recent editions of the two most widely used browsers, Microsoft Internet Explorer and Netscape Navigator®. Acquirers, merchants, and issuers may elect to support other browsers on a variety of platforms such as WAP browsers on wireless devices or voice recognition over land or wireless connections.

Magnetic Stripe Cardholders

Prerequisites

For cardholders with magnetic stripe cards, the only prerequisite to using 3-D Secure is enrollment with the card issuer.

Enrollment

To enroll, the cardholder must supply identification information to an issuer enrollment service (such as a Web-based service or a personal service in a branch or service center) to enable the issuer to confirm the cardholder's identity. Depending on the authentication method selected by the issuer for purchase transactions, the cardholder may be asked to select a password, and possibly a hint and response to use in the event the password is forgotten.

Additionally, the cardholder may be asked to select a Personal Assurance Message, which will be displayed on the Purchase Authentication Page when the cardholder is asked to supply authentication information (such as a password). The Personal Assurance Message enables the cardholder to know that the Purchase Authentication Page is from their card issuer.

Having completed enrollment, a cardholder is ready to shop using 3-D Secure.

Purchase

The cardholder shops, selecting goods and services to purchase from a merchant Web site. After shopping, the cardholder starts the merchant checkout process and responds to merchant questions about shipping and billing details, payment card number, and so on.

The merchants' questions can be answered either directly on screens provided by the merchant or through an electronic wallet, merchant expedited checkout, or other service.

If the issuer offers or sponsors an electronic wallet or a server-based checkout completion service, the cardholder must complete other preparation processes to use such services, such as additional enrollment steps and installation of software. See Chapter 7, Member and Merchant Implementation Considerations for more information on wallets.

Chip Cardholders

Prerequisites

Issuers may choose to authenticate their chip cardholders for 3-D Secure without requiring the use of a card reader, in which case the description in section, "*Magnetic Stripe Cardholders*" applies.

To enable authentication of the chip card as well as the cardholder, the prerequisites for using 3-D Secure are:

- Enrollment with the card issuer, and
- An appropriate chip card reader and supporting software (typically supplied by the chip card issuer).

Enrollment

Depending upon the support offered by the chip card issuer, the cardholder may need to be involved in such tasks as locating and purchasing a certified card reader, downloading or otherwise procuring issuer-approved or issuer-supplied software, and installing the hardware and software.

An issuer that intends to offer chip card authentication should carefully plan so as to minimize demands on the cardholder and maximize the potential for cardholder success.

- Cardholder Web support or dial-up support sites could increase success and customer satisfaction.
- Vendors may prepare packaged offerings for issuers that facilitate the hardware and software selection and installation process.
- Issuers may offer a complete chip card package that includes an issuer-branded card reader, software, and simple instructions for installation.

To support payment authentication using chip card, cardholders may need to install additional software and hardware, may need prerequisite versions or brands of platform or special software, or both. See more details in Chapter 8, Issuer Implementation Considerations*,* section*,* "Cardholder Hardware and Software*."*

Member and Merchant Implementation Considerations 7

Purpose

This chapter describes some implementation considerations that apply to Visa members, merchants, and third parties that will plan, implement, and operate 3-D Secure systems.

Additional considerations for issuers are discussed in Chapter 8, Issuer Implementation Considerations; additional considerations for acquirers and merchants are discussed in Chapter 9, Acquirer and Merchant Implementation Considerations.

Wallets

Wallets that perform form fill-in, account number recall, key storage, password storage, and other functions are available from a variety of solution providers.

Visa members may choose to supply or support cardholder wallets to facilitate shopping, or to facilitate the use of virtual or pseudo-numbers for the protection of card numbers; issuers may choose to supply or support cardholder wallets to enable authentication technologies such as public key certificates.

To the extent they do, members may become involved in wallet distribution and support, and may need to incorporate changes in their software. For instance, an issuer may choose to incorporate support in the ACS for cardholder wallets to be used during the authentication process.

Additional information is available from the vendors of wallet products.

Mobile Device Support

3-D Secure is defined to be extensible in order to support cardholders using a variety of access devices and channels. Currently, two extensions have been defined to support cardholders using mobile devices. Visa is also developing extensions to support other environments. Issuers and merchants interested in supporting additional devices and channels should contact their Visa representatives.

For more information about payment authentication using mobile Internet devices, such as WAP phones, see:

- *3-D Secure: Protocol Specification – Extension for Mobile Internet Devices, Visa Publication 70006-01 (licensed)*

For more information about payment authentication using SMS, USSD, or voice/IVR, see:

- *3-D Secure: Protocol Specification – Extension for Voice and Messaging Channels, Visa Publication 70004-01 (licensed)*

Issuer Implementation Considerations 8

Purpose

This chapter describes some important considerations for issuers and third parties that will plan, implement, and operate 3-D Secure systems.

This chapter provides the reader with a general understanding of the scope and tasks involved in a 3-D Secure implementation, the variety of options and alternatives that must be considered, and the major decisions that must be made during planning and implementation.

Available Documentation

The 3-D Secure publication suite includes:

- 3-D Secure: Implementation Guide – Issuer, Visa Publication 70013-01
- 3-D Secure: Security Requirements – Enrollment and Access Control Servers, Visa Publication 70016-01 (licensed)

These documents are intended to assist issuers to:

- Understand the functions, usage, and benefits of 3-D Secure,
- Develop strategies that will achieve issuer objectives for cardholder enrollment and other marketing goals; and
- Establish and guide the activities of a project responsible for successfully planning, developing, testing, and launching the 3-D Secure service offering.

Implementation Project

Once the decision is made to implement 3-D Secure, the issuer should establish an implementation project team and prepare an implementation plan.

Project Team

The project team should be multidisciplinary and include both a business manager and a project manager. Among the functions that should be represented are marketing, legal, compliance, operations, customer support, risk, and information technology.

Project Tasks

Project tasks include:

- Establish business objectives
- Select underlying technology (build, buy, or use Visa enabling services)
- Identify initial cardholders
- Select enrollment methodology
- Plan customer support
- Develop cardholder enrollment facilities
- Establish customer support policies and procedures
- Plan to modify dispute resolution procedures
- Incorporate 3-D Secure processing components, changes, and policies into existing information infrastructure
- Develop marketing plans and strategy including Graphical User Interface (GUI) design and solicitation materials
- Specify initial card number ranges to support
- Generate keys and acquire digital certificates
- Satisfy security requirements to obtain Visa approval to activate servers
- Conduct pilot (generally with employees functioning as cardholders)
- Execute production rollout plans
- Monitor program operation

Enrollment Server

Selecting the Enrollment Server

An issuer can build or buy software to support an Enrollment Server, or may use the Visa enabling service for 3-D Secure enrollment if offered by its Visa region. An issuer may have an existing system suitable to be enhanced to perform the enrollment services, such as a home banking enrollment server. Vendors may offer customizable Enrollment Server solutions.

NOTE: *The issuer must comply with the requirements in:*

3-D Secure: Security Requirements – Enrollment and Access Control Servers, Visa Publication 70016-01 (licensed)

Cardholder Impact

If the issuer offers online enrollment, aside from information appearing on the issuer's Web site, the Enrollment Server will be the first point of online contact with the issuer's 3-D Secure services.

Contact with the Enrollment Server is an early opportunity for the issuer to begin cardholder education, to provide additional marketing and technical information, to provide support contacts, and – in the case of cardholders planning to use authentication methods such as chip card or mobile devices – to provide software and hardware offerings and specifications.

Tailoring to Various Platforms

The issuer should consider whether it would be beneficial to optimize the Enrollment Server appearance and performance for popular browsers running on specific platforms.

Access Control Server

Selecting the Access Control Server

An issuer can build or buy software to support an Access Control Server (ACS) and/or attempts functionality, or may use the Visa enabling service for 3-D Secure access control and/or attempts functionality, to the extent one or both are offered by its Visa Region. An issuer may have an existing system suitable to be enhanced to perform the access control services. Vendors may offer customizable Access Control Server software, integrated hardware and software solutions, third-party hosting, or complete third-party ACS services.

Developing an Access Control Server

An issuer that decides to develop an internal custom Access Control Server will need to refer to the following publications:

- *3-D Secure: Protocol Specification – Core Functions, Visa Publication 70000-01 (licensed)*
- *3-D Secure: Functional Requirements – Access Control Server, Visa Publication 70002-01 (licensed)*
- *3-D Secure: Security Requirements – Enrollment and Access Control Servers, Visa Publication 70016-01 (licensed)*

If plans include chip card authentication or mobile device support then the issuer should also refer as appropriate to:

- *3-D Secure: Functional Specification – Chip Card Authentication, Visa Publication 70005-01 (licensed)*
- *3-D Secure: Protocol Specification – Extension for Mobile Internet Devices, Visa Publication 70006-01 (licensed)*
- *3-D Secure: Protocol Specification – Extension for Voice and Messaging Channels, Visa Publication 70004-01 (licensed)*

For additional information regarding required compliance testing of the Access Control Server, the issuer should refer to all of the documents listed in Chapter 2, 3-D Secure Publication Suite, section, "Compliance Publications."

In addition to meeting the general planning steps described in section, *Project Tasks*, the issuer must satisfy the detailed protocol, design, and compliance requirements in the documents listed on page 8-5, and complete other specific tasks for ACS development including:

- Design customized GUI (Graphical User Interface) for cardholder interaction
- Choose and provide the URL (Uniform Resource Locator)
- Define the overall authentication process, including such matters as:
  - What method or methods of cardholder authentication to support
  - Define policies and threshold criteria for successful authentication
- Generate keys and obtain digital certificates
- Perform Visa compliance testing
- Meet the Visa requirements to secure approval to activate the Access Control Server
- Perform Visa acceptance testing
- Perform in-house issuer acceptance testing
- Execute production rollout plans
- Monitor operation of the ACS

Product Integration Testing

The PIT is a remote Web-testing environment that provides the equivalent of all components of the 3-D Secure infrastructure. The PIT provides issuers (and issuer processors) and vendors with a facility for production readiness testing of ACS implementations. All new ACS implementations must successfully complete Product Integration Testing prior to entering the productions 3-D Secure service.

PIT allows Visa to verify that compliant 3-D Secure ACS components integrated at issuer or issuer processor sites comply with all processing requirements of 3-D Secure and are production ready.

Customer Support

Selecting the Customer Support Option

An issuer that plans to use the Visa enabling services has two customer support options:

1. Provide first contact (Level 1) customer support themselves and rely upon Visa for issuer (Level 2) support and Application (Level 3) support
2. Provide all customer support or contract with a third party to provide support.

Visa recommends that issuers select the first option.

Issuer Customer Support

Except as described above, the issuer is responsible for customer support for 3-D Secure. After reviewing the 3-D Secure customer support requirements to determine how well they fit with the issuer's existing customer support strategy, operation, and policies, issuers should attempt to integrate 3-D Secure support with other card product areas.

The issuer must decide to what extent to use the issuer's existing customer support, Visa customer support for enabling services, or third-party support and over what channels to offer support. If multiple entities or organizations are providing support, a well-planned and executed escalation and incident transfer system is essential.

When choosing how to configure customer support, issuers should consider such matters as:

- Their Internet experience, capability, and capacity;
- Their ability to manage e-mail communications with customers; and
- The need for 24x7 availability of customer support for e-commerce and how to achieve that availability.

Authentication Methods

Authentication Technologies

Visa recognizes that deciding the appropriate means of authentication is best left to the issuer, based on the issuer's assessment of the risk of each transaction. The core protocol describes the use of a password for authentication; the chip card functional specification describes authentication using a chip card. Additional technologies may be acceptable in various regions and for particular purposes, such as support for mobile devices. However, Visa regions may establish rules that require members to review their proposed authentication technologies with their Visa region. Issuers should consult their Visa representatives for details.

Multiple Authentication Methods

Chip cards are becoming widely available products. They can be used as a means of enhancing the validation of cardholders during the 3-D Secure enrollment process and during 3-D Secure payment transactions.

In 3-D Secure the chip card (specifically the Visa Smart Debit/Credit card) can be deployed by the issuer as a second factor to enhance the strength of authentication decisions, and for validating cardholder enrollment. Issuers using chip card authentication can be sure that the chip card was inserted in a card reader at the cardholder client system at the time of the purchase.

For more detailed information about deploying chip cards to enhance authentication in 3-D Secure, see:

3-D Secure: Functional Specification – Chip Card Authentication, Visa Publication 70005-01 (licensed)

Cardholder Hardware and Software

Cardholder Software for Password Authentication

If issuers choose to deploy the password-based authentication technology described in 3-D Secure core protocol (see page 11), then no specialized hardware or software or installation process is required for cardholders. The cardholder should have a personal computer or other device that runs a version of one of several widely available browsers such as Microsoft Internet Explorer or Netscape Navigator. Other browsers may also work. Issuers should determine the list of browsers for which they intend to provide support and publish that list to cardholders.

Cardholder Hardware and Software for Chip Card

To support chip card authentication, the cardholder must have a properly equipped platform including a card reader, a card reader device driver, and a terminal program.

If the issuer decides to support chip card, the 3-D Secure project plan should be expanded to include chip card and chip card experts should be added to the implementation team. Implementation choices include:

- Whether to provide card readers and driver software to cardholders or provide a list of compliant card readers and driver software
- Whether to develop custom terminal software, contract, or buy off the shelf products
- Whether to support public access points such as kiosks where cardholders can use their chip cards
- How much and what kind of additional customer technical support to supply
- What additional marketing and solicitation materials to produce

As with other issuer components, the cardholder client terminal software must complete the Visa compliance process and be acknowledged by Visa before it can be provided to cardholders and used.

For more details, please refer to:

- *3-D Secure: Functional Specification – Chip Card Authentication, Visa Publication 70005-01 (licensed)*
- *3-D Secure: Security Requirements – Enrollment and Access Control Servers, Visa Publication 70016-01 (licensed)*

Acquirer and Merchant Implementation Considerations 9

Purpose

This chapter describes some important considerations for acquirers, merchants, and third parties that will plan, implement, and operate 3-D Secure systems.

This chapter provides the reader with a general understanding of the scope and tasks involved in a 3-D Secure implementation, the variety of options and alternatives that must be considered, and the major decisions that must be made during planning and implementation.

Merchant Authentication

For information on merchant authentication, see Chapter 4, Security, “Merchant Authentication.”

Impact of Issuer Choices

The card products an issuer chooses to support do not affect the merchant, nor do the authentication methods that issuers select. After the issuer Access Control Server processes a payment authentication request, it sends a response to the merchant indicating whether authentication was successful. There is no impact on the merchant as a result of the issuer’s authentication method or policies.

Available Documentation

The 3-D Secure publication suite includes:

3-D Secure: Implementation Guide – Acquirer, Visa Publication 70014-01

3-D Secure: Implementation Guide – Merchant, Visa Publication 70020-01

These guides are intended to assist acquirers and merchants to:

- Understand the functions, usage, and benefits of 3-D Secure,
- Develop strategies that will achieve acquirer objectives for merchant participation and other marketing goals; and
- Establish and guide the activities of a project responsible for successfully planning, developing, testing, and launching the 3-D Secure service offering.

Merchants, acquirers, and third parties that intend to develop a Merchant Server Plug-in should also consult:

3-D Secure: Functional Requirements – Merchant Server Plug-in, Visa Publication 70003-01 (licensed)

Planning

Implementation Guides

In addition to the 3-D Secure publication suite described in Chapter 2, in Table 2–1, there is a set of 3-D Secure Implementation Guides available only to Visa members. Members who need these guides should consult their Visa representative.

Project Team

Prior to implementing 3-D Secure, a merchant or acquirer will want to establish a multidisciplinary project team, including both a business manager and a project manager. Among the functions that should be represented on the team are marketing, legal, compliance, operations, customer support, risk, and information technology.

Implementation Plan

Prepare an implementation plan that includes:

- Software solution selection – build, buy from solution providers, or use third-party services (see discussion below)
- Development and installation
- Visa compliance testing
- Testing and integration
- Execute production rollout plans

Analysis and Product Selection

Consider merchant technological capabilities, size, business requirements, and benefits with the objective of deciding what general approach the merchant should take to establish the functional capabilities necessary to participate in 3-D Secure. Implementation alternatives include:

- Integrating components purchased from a solution provider into an existing system
- Using or integrating services from a third-party payment services provider
- Using a complete storefront package developed by a third party
- Participating or subscribing to complete services provided by a third party, such as a mall operator

- Developing a custom internal or contracted system

NOTE: *All 3-D Secure products, regardless of source, must complete compliance testing as described in the documents listed in Chapter 2, 3-D Secure Publication Suite, section, "Compliance Publications."*

Merchant Server Plug-in

Functions

The Merchant Server Plug-in (MPI) is a key component of the 3-D Secure solution. It is software that is integrated with a merchant's Web storefront software, or supplied as a service for merchants by an acquirer or payment service provider. It performs essential functions in processing a 3-D Secure authentication transaction including:

- Transmitting cardholder enrollment inquiries to the Visa Directory Server
- Receiving cardholder enrollment responses from the Visa Directory Server
- Transmitting authentication requests via the cardholder browser to the ACS
- Receiving authentication responses via the cardholder browser from the ACS
- Validating the cryptographic signature in the response message from the ACS to ensure the authenticity and integrity of the response
- Providing data to the merchant's authorization processing function
- Optionally, collecting and reporting on statistical information about authentication processing

Validating Digital Signature

When an authentication response message is returned via the cardholder system to the merchant, the issuer's digital signature in that response must be validated to ensure the authenticity and integrity of the message. Signature validation requires a Visa-issued certificate (which is received with the signed message) and the ability to perform the necessary cryptographic signature verification calculations.

This function may be performed as an integral part of the MPI or by a Validation Server, which an acquirer or third party may offer as a service. Acquirers that decide to offer this service must decide whether to build or buy the software and hardware, or to contract with a third party to provide the service.

Acquirers or payment processors that choose to provide remote MPI services may also offer integrated validation services.

Architecture

The MPI may be implemented in a variety of ways, ranging from a wholly integrated software component to a group of distributed components or services providing discrete functions such as ACS signature validation, request and response preparation, Visa Directory Server interfaces, and statistical and reporting functions.

As mentioned previously, the MPI need not be co-located with the merchant transaction server, and all or part of its functions may be offered by an acquirer or payment processor as a remote service.

Developing an MPI

Merchants, acquirers, and third parties that intend to develop an MPI should consult:

3-D Secure: Functional Requirements – Merchant Server Plug-in, Visa Publication 70003-01 (licensed)

Merchant Software Changes

For merchants already engaged in e-commerce, the changes to existing storefront software should be straightforward, since they are already collecting most, if not all, required information. In addition, they have already established interfaces to acquirers or payment service providers to process authorizations.

Changes to the merchant e-commerce site must be made to integrate the MPI.

Required Changes

After the cardholder provides the card number and signals willingness to buy, the merchant storefront software must pass control and information to a component or service that performs the functions of the MPI.

After the authentication response is received, the MPI may either:

- Pass control back to the merchant software that handles authorization requests; or
- Format and submit the authorization request, then pass control back to the merchant software.

In either case, the merchant software may require changes.

Changes That May Be Required

Various changes may be required as a result of the current merchant software. For example:

- If the current storefront software does not collect all necessary information from the cardholder to prepare 3-D Secure request messages, changes must be made to enable collecting that data.
- Adjustments to the process of preparing an authorization request to incorporate data from the authentication response (See section, ”CAVV, ECI, and XID” for further information.)
- It may be necessary to adjust the current software to deal with exceptions.

The acquirer or the Visa region may mandate other changes. These include:

- Preparing customized Web pages for 3-D Secure that conform to content and placement guidelines, including use of service marks.

Optional Changes

A merchant may choose to provide additional support for 3-D Secure, such as:

- Customizing exception handling
- Changing the storefront software to indicate that 3-D Secure is supported

CAVV, ECI, and XID

Depending on the requirements of the Visa region, merchants and acquirers will have to transmit values in the following three data fields listed in Table 9–1 in the authorization message submitted into VisaNet following receipt of a payment authentication request representing a transaction in which cardholder authentication was successful or one in which proof of an authentication attempt was performed.

Table 9–1: 3-D Secure Fields for Authorization Request

CAVV	If the authentication is successful, the ACS creates a cryptographic control value called the Cardholder Authentication Verification Value (CAVV), which provides the ability for VisaNet to independently validate the integrity of important fields from the authentication response, which are included in the authorization message.
ECI	Electronic Commerce Indicator
XID	Transaction Identifier (this field is optional as of 5 April 2003)

Platform Selection

The merchant platform must meet the compliance requirements specified in:

3-D Secure: Compliance Testing Facility – Policies and Procedures, Visa Publication 70017-01

3-D Secure: Compliance Testing Facility – Test Scripts, Visa Publication 70019-01 (licensed)

In addition, the merchant platform must meet the functional and technological requirements to correctly interface with a MPI and the contractual requirements of the acquirer with which the merchant is affiliated.

The functional requirements for the MPI were developed in the context of a general understanding of mainstream operating system, Web server, and storefront development environments to enable development of software that is widely compatible with products being used by most merchant sites. It is not expected that platform selection will be a significant issue for merchants or acquirers.

Merchant Implementation

Merchant Implementation Steps

While there are a number of steps to be managed in the process of a merchant implementation, they are all well within the state of practice in Web site development and maintenance.

Following is a brief list of the steps:

Storefront Changes: As discussed in section, "Merchant Software Changes" may include:

- Identify the site as 3-D Secure enabled
- Collect any additional information required by 3-D Secure
- Prepare customized pages
- Design and implement interfaces to the selected MPI

Install Plug-in:

- Integrate the MPI with the merchant platform, Web server, and other site software; or
- Determine where and how to connect to acquirer or payment processor MPI service.

Obtain SSL/TLS Certificate: Whichever entity will operate the MPI – merchant, acquirer, or third party – will require an SSL/TLS server certificate for secure cardholder communication sessions.

- Typically, a merchant with an existing Web site will have obtained such certificates in the ordinary course of business.
- If an acquirer or third party will operate the MPI, or if the merchant does not yet have an SSL/TLS server certificate, the entity that will operate the MPI must obtain the certificate.

Merchant Authentication: For authenticating a merchant to the Visa Directory Server, it is necessary for the merchant to obtain a certificate or a merchant ID and password from its acquirer. Acquirers should ask their Visa representative about regional requirements for certificates or merchant ID and password.

Configuration: Changes to server configurations, DNS, routing tables, firewalls, procedures, and other operational matters.

Testing: Configuration and acceptance testing as required by the merchant's internal acceptance process and the acquirer.

Compliance Testing: The entity that developed the MPI obtains an *acknowledgement of compliance* indicating that they have completed compliance testing as described in the documents listed in Chapter 2, 3-D Secure Publication Suite, section, “Compliance Publications.” (If the MPI is obtained from a third party or from the acquirer, this testing may have been completed previously but it remains the responsibility of the entity intending to use the MPI to ensure the testing was performed and properly acknowledged.)

Production: Final steps necessary to connect merchant systems to live 3-D Secure environment and activate.

Product Integration Testing (PIT)

The PIT is a remote Web-testing environment that provides the equivalent of all components of the 3-D Secure infrastructure. The PIT provides acquirers (and acquirer processors), merchants (and merchant aggregators), and vendors with a facility for production readiness testing of MPI component implementations. All new MPI implementations must successfully complete Product Integration Testing prior to entering the production 3-D Secure service.

PIT allows Visa to verify that compliant 3-D Secure MPI components integrated at merchant or merchant aggregator sites comply with all processing requirements of 3-D Secure and are production ready.

Merchant Training and Support

If the acquirer provides MPIs or related components or services to merchants, it is the acquirer’s responsibility to provide appropriate training and support. Acquirers may rely on solution providers to perform this function.

Merchants are responsible for the training and support of their own personnel in operating and administering their Web sites and dealing with customer questions about how their shopping and purchasing facilities operate.

Glossary

The terminology, acronyms, and abbreviations below are used in this and other documents in the 3-D Secure publication suite.

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.

3-D Secure specifications

Refers to the Protocol Specification and Functional Requirements documents described in Chapter 2, 3-D Secure Publication Suite, section, “Product Publications.”

Access Control Server (ACS)

A component that operates in the Issuer Domain, verifies whether authentication is available for a card number, and authenticates specific transactions.

Account Information Security Program (AISP)

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 member financial institution that establishes a contractual service relationship with a merchant for the purpose of accepting Visa cards. In 3-D Secure, the acquirer determines whether the merchant is eligible to participate. Performs the traditional role of receiving and forwarding authorization and settlement messages (enters the transaction into interchange).

Acquirer Domain

Contains the systems and functions of the acquirer and its customers, such as merchants.

ACS

See Access Control Server.

AHS

See Authentication History Server.

AISP

Visa Account Information Security Program

attempts functionality

The process by which the proof of an authentication attempt is generated when payment authentication is not available.

Authenticated Payment Program

One of the programs of the Visa Secure e-Commerce Initiative, this program includes two authentication protocols: 3-D Secure and 3-D SET.

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

A process by which an issuer, or a processor on the issuer's behalf, approves a transaction for payment.

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.

In 3-D Secure, it 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).

CAD

Card Acceptance Device

Card Acceptance Device

A device capable of reading a magnetic stripe or chip card. See also card reader.

card reader

See chip card reader.

cardholder

Party that holds a Visa payment card, shops, provides card number, and commits to payment.

Cardholder Authentication Verification Value (CAVV)

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 (PARes) 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).

Cardholder Client System

Refers to the system environment within which the cardholder uses 3-D Secure, such as a personal computer, a set top box, or a mobile phone, including the browser software, terminal software if required, and card reader if required.

cardholder software

Optional cardholder software that may supplement the abilities of the browser. Chip card authentication, for example, requires cardholder software sometimes referred to as terminal software.

CAVV

See 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 unforgeable by cryptographic technology (signing with the private key of the certificate authority).

certificate authority

A trusted party that issues and revokes certificates.

chip

An integrated circuit containing memory and logic where a copy of the VSDC application is stored and executed.

chip card

A payment card with an integrated circuit chip that stores information about the account and user.

chip card reader

The electromechanical device into which a chip card is inserted for use with a terminal application; functionally equivalent to the Card Acceptance Device (CAD) or InterFace Device (IFD). In the personal computer environment such a device does not typically incorporate an integrated numeric keypad, though in the set top box or mobile phone environment a numeric keypad is typically integrated.

core protocol

Refers to the protocol described in the publication: 3-D Secure: Protocol Specifications – Core Functions, Visa Publication 70000-01

CRReq

Card Range Request

CRRes

Card Range Response

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 certificate

See certificate.

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.

digital wallet

A software component that allows a user to make an electronic payment with a financial instrument (such as a credit card) while hiding the low-level details of executing the payment protocol, including such tasks as entering an account number and providing shipping information and cardholder identifying information.

Directory Server

See Visa Directory Server.

Enrollment Server

Operates in the Issuer Domain; a server hardware/software entity which manages cardholder enrollment 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.

Graphical User Interface

Refers to what the user sees on the display screen, including the arrangement and composition of elements such as pictures, buttons and other application controls, windows, selection lists, and scroll bars.

GUI

Graphical User Interface

Hardware Security Module (HSM)

A secure hardware device that stores cryptographic keys and performs cryptographic functions such as encrypting/decrypting data streams.

HTML

Hypertext Markup Language, a computer programming language used to define pages on the World Wide Web.

Interoperability Domain

Facilitates the transfer of information between the Issuer and Acquirer Domain systems.

Issuer

A Visa member financial institution that issues Visa cards, contracts with cardholder to provide card services, determines eligibility of cardholder to participate in 3-D Secure, and identifies card number ranges eligible to participate in 3-D Secure.

Issuer Domain

Contains the systems and functions of the issuer and its customers (cardholders).

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.

magnetic stripe

The stripe on the back of a payment card that contains electro-magnetically encoded account information required to complete a transaction.

merchant

Entity that contracts with an acquirer to accept Visa cards and manages the online shopping experience with the cardholder, obtains card number, then transfers control to the Merchant Server Plug-in, which conducts payment authentication.

Merchant Server Plug-in (MPI)

A component that operates in the Acquirer Domain; incorporated into the merchant's Web storefront to perform functions related to 3-D Secure on behalf of the merchant, such as determining whether authentication is available for a card number and validating the digital signature in a 3-D Secure message.

MPI

See Merchant Server Plug-in.

offline PIN verification

A process whereby a chip card is validated using RSA public key technology to protect against counterfeiting or skimming.

PAReq

See Payer Authentication Request.

PARes

See Payer Authentication Response.

Payer Authentication Request (PAReq)

A message sent from the Merchant Server Plug-in to the 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.

See PAReq and CPRQ.

Payer Authentication Response (PARes)

A message formatted, digitally signed, and sent from the 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.

See PARes and CPRS.

private key

Part of an asymmetric cryptographic system. The key that is kept secret and known only to an owner.

public key

Part of an asymmetric cryptographic system. The key known to all parties.

Public Key Infrastructure

Provides the core framework for a wide variety of components, applications, policies, and practices to be combined to achieve operational and practical public-key based security functions for commercial transactions.

public key pair

Two mathematically related keys – a public key and a private key – which are used with a public key (asymmetric) cryptographic algorithm to permit the secure exchange of information without the necessity for a secure exchange of a secret.

secret key

A key used in a symmetric cryptographic algorithm such as DES, which if disclosed publicly, would compromise the security of the system.

Secure e-Commerce Initiative

A Visa initiative focused on increasing e-commerce transactions, promoting consumer confidence, and increasing member and merchant profitability, and including the following programs:

- Visa Account Information Security Program
- Visa Authenticated Payment Program (which includes 3-D Secure)
- Best Business Practices Program

Secure Sockets Layer

SSL: A cryptographic protocol developed by Netscape Communications Company to confidentially transmit information over open networks like the Internet. See also Transport Layer Security.

SET

SET Secure Electronic Transaction™, one of the two protocols approved for the Authenticated Payment Program.

smart card

See chip card.

specifications

See 3-D Secure specifications.

SSL

See Secure Sockets Layer.

Three-Domain Secure

See 3-D Secure.

TLS

See Transport Layer Security.

Transport Layer Security

Successor protocol to SSL developed by the IETF (Internet Engineering Task Force).

Uniform Resource Locator (URL)

Address scheme for pages on the World Wide Web usually in the format http://address or https://address such as http://www.visa.com.

URL

See Uniform Resource Locator.

Validation

Usually refers to validating the cryptographic signature passed in the message from the ACS to the merchant.

VEReq

See Verify Enrollment Request.

VERes

See Verify Enrollment Response.

Verify Enrollment Request

Message from Merchant Server Plug-in to the Visa Directory Server or from Visa Directory Server to the ACS, asking whether authentication is available for a particular card number.

Verify Enrollment Response

Message from the ACS or the Visa Directory Server, telling the Merchant Server Plug-in whether authentication is available.

Visa Directory Server

A server hardware/software entity which is operated by Visa in the Interoperability Domain; it processes CRReq and VEReq messages and creates CRReq and (in some situations) VERes messages.

Visa Certificate Authority

A component that operates in the Interoperability Domain and that generates and distributes selected digital certificates to entities participating in 3-D Secure.

VisaNet

The systems and services, including the V.I.P. and BASE II systems, through which Visa delivers online financial processing, authorization, and clearing and settlement services to members.

wallet

See digital wallet.

WAP

Wireless Application Protocol

Wireless Application Protocol (WAP)

An open, global specification for a communications and application protocol to exchange information and services with wireless devices.