



# MasterCard *SecureCode*

Merchant Implementation Guide

9 November 2011

---

## Notices

### Proprietary Rights

The information contained in this document is proprietary and confidential to MasterCard International Incorporated, one or more of its affiliated entities (collectively “MasterCard”), or both.

This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of MasterCard.

### Trademarks

Trademark notices and symbols used in this document reflect the registration status of MasterCard trademarks in the United States. Please consult with the Customer Operations Services team or the MasterCard Law Department for the registration status of particular product, program, or service names outside the United States.

All third-party product and service names are trademarks or registered trademarks of their respective owners.

### Billing

For printed documents, MasterCard will bill principal members. Please refer to the appropriate *MasterCard Consolidated Billing System* (MCBS) document for billing-related information.

### Information Available Online

MasterCard provides details about the standards used for this document—including times expressed, language use, and contact information—on the Member Publications Support page available on MasterCard OnLine®. Go to Member Publications Support for centralized information.

### Translation

A translation of any MasterCard manual, bulletin, release, or other MasterCard document into a language other than English is intended solely as a convenience to MasterCard members and other customers. MasterCard provides any translated document to its members and other customers “AS IS” and makes no representations or warranties of any kind with respect to the translated document, including, but not limited to, its accuracy or reliability. In no event shall MasterCard be liable for any damages resulting from members’ and other customers’ reliance on any translated document. The English version of any MasterCard document will take precedence over any translated version in any legal proceeding.

### Publication Code

SMI

---

## Summary of Changes, 9 November 2011

To locate changes online, on the Adobe toolbar, click Find. In the Find box, type \*chg\*, and then press ENTER. To move to the next change, press ENTER again.

Description of Change	Where to Look
To ensure that members have access to current contact information and standards used for MasterCard documentation, MasterCard has created the Member Publications Support page. As a result, MasterCard has removed some content from this document, including times expressed, language use, and contact information, which members now can find online.	Member Publications Support page on MasterCard OnLine®
Updated the following sections: <ul style="list-style-type: none"><li>• <a href="#">Grow Your Online Business</a></li><li>• <a href="#">Merchant Plug-In</a></li></ul>	<a href="#">Chapter 1</a>
Updated the <a href="#">Card Range Request/Response</a> section.	<a href="#">Chapter 2</a>
Updated the following sections: <ul style="list-style-type: none"><li>• <a href="#">General Responsibilities</a></li><li>• <a href="#">AAV Usage</a></li><li>• <a href="#">Passing the Electronic Commerce Indicator in the Authorization Message</a></li><li>• <a href="#">Recurring Payments</a></li><li>• <a href="#">Maestro Considerations</a></li><li>• <a href="#">Creation of Cardholder Authentication Window</a></li><li>• <a href="#">Cache Expiration Timers</a></li><li>• <a href="#">Zero or Empty Parameters</a></li></ul>	<a href="#">Chapter 4</a>
Updated Contact Information.	<a href="#">Appendix C</a>
Added two new appendices: <ul style="list-style-type: none"><li>• <a href="#">India IVR Transactions (SecureTelephone)</a></li><li>• <a href="#">MasterCard Advance Registration Program</a></li></ul>	<ul style="list-style-type: none"><li>• <a href="#">Appendix E</a></li><li>• <a href="#">Appendix F</a></li></ul>
Updated verbiage and graphics where appropriate.	Throughout Manual

---

# Table of Contents

<b>Chapter 1 Overview .....</b>	<b>1-i</b>
MasterCard and Electronic Commerce .....	1-1
Maestro and Electronic Commerce .....	1-1
Grow Your Online Business .....	1-2
MasterCard <i>SecureCode</i> Platform Components .....	1-3
Universal Cardholder Authentication Field and its Structure .....	1-3
Accountholder Authentication Value .....	1-4
Merchant Plug-In .....	1-4
<b>Chapter 2 SecureCode 3-D Secure Solution.....</b>	<b>2-i</b>
Overview .....	2-1
Components.....	2-1
Issuer Domain.....	2-1
Acquirer Domain .....	2-2
Interoperability Domain.....	2-3
Messages.....	2-4
Card Range Request/Response .....	2-4
Verification Request/Response.....	2-4
Payer Authentication Request/Response.....	2-4
Payer Authentication Transaction Request/Response .....	2-5
Cardholder Enrollment.....	2-5
Cardholder Enrollment Process.....	2-5
Sample Cardholder Enrollment Flow .....	2-6
Cardholder Authentication .....	2-11
Sample Cardholder Authentication Process .....	2-11
Sample Cardholder Authentication Flow .....	2-13
<b>Chapter 3 Component Certificate Requirements and Authentication Options .....</b>	<b>3-i</b>
Overview .....	3-1
Functional Certificate Authority Hierarchy.....	3-1
Public Zone .....	3-2
Trusted Zone .....	3-2
Operational Certificate Authority Hierarchy.....	3-3
Certificates .....	3-4
Requesting Certificates.....	3-6

<b>Chapter 4 Merchants</b> .....	<b>4-i</b>
Overview .....	4-1
General Responsibilities.....	4-1
Infrastructure .....	4-1
Establishment of MasterCard <i>SecureCode</i> Operating Environment .....	4-2
Authorization System Enhancements .....	4-2
Maestro Considerations.....	4-5
Customization .....	4-5
Program Identifier Usage Guidelines .....	4-5
Integrated Support for Merchant Plug-In Processing .....	4-6
Consumer Message on Payment Page .....	4-8
Creation of Cardholder Authentication Window.....	4-8
TERMURL Field.....	4-9
Replay Detection .....	4-9
Merchant Server Plug-In Configuration.....	4-10
Operational.....	4-12
Loading of MasterCard Root Certificates .....	4-12
Loading of MasterCard SSL Client Certificate .....	4-12
MPI Log Monitoring.....	4-12
MPI Authentication Request/Response Archival .....	4-12
Accountholder Authentication Value (AAV) Processing .....	4-13
Identification of SPA AAV Format in PAREs.....	4-13
Validation of Payer Authentication Response (PAREs) Signature .....	4-13
Global Infrastructure Testing Requirements.....	4-13
MasterCard Site Data Protection Program .....	4-13
Merchant Processing Matrix .....	4-14
Formatted File Type.....	4-14
<b>Appendix A Merchant Customer Service Guide</b> .....	<b>A-i</b>
Frequently Asked Questions.....	A-1
MasterCard <i>SecureCode</i> .....	A-1
Cardholder Enrollment.....	A-5
Traditional Cardholder Enrollment .....	A-5
Activation During Shopping .....	A-6
Consumer Buying Scenarios .....	A-6
Authentication—Successful.....	A-7
Authentication—Forgotten MasterCard <i>SecureCode</i> .....	A-8
Authentication—Failed .....	A-9
Authentication—Account Locked .....	A-10
Activation During Shopping (ADS).....	A-11

---

Activation During Shopping—Opt Out of Enrollment .....	A-12
<b>Appendix B MasterCard SecureCode SPA Algorithm Specifications .....</b>	<b>B-i</b>
Overview .....	B-1
Accountholder Authentication Value Layout .....	B-1
Base64 Encoding .....	B-1
Introduction .....	B-1
Examples .....	B-2
Base64 Alphabet .....	B-3
<b>Appendix C Contact Information .....</b>	<b>C-i</b>
Contact Information .....	C-1
MasterCard <i>SecureCode</i> Online Resources .....	C-1
<b>Appendix D Maestro Considerations .....</b>	<b>D-i</b>
Account in Good Standing .....	D-1
<b>Appendix E India IVR Transactions (SecureTelephone) .....</b>	<b>E-i</b>
Overview .....	E-1
Data Extensions to the existing 3-D Secure Protocol .....	E-1
UCAF Transport in MasterCard Authorization Messages .....	E-1
MasterCard <i>SecureCode</i> —Security Level Indicator (DE 48, subelement 42) .....	E-2
Universal Cardholder Authentication Field (DE 48, subelement 43) .....	E-2
<b>Appendix F MasterCard Advance Registration Program .....</b>	<b>F-i</b>
MasterCard Advance Registration Program .....	F-1
Participation Requirements for Merchants .....	F-1
MARF Merchant Use of MasterCard <i>SecureCode</i> .....	F-2
Acquirer Impact .....	F-3

---

# Chapter 1 Overview

*This section provides a general overview of the MasterCard® SecureCode™ Electronic Commerce program.*

---

MasterCard and Electronic Commerce .....	1-1
Maestro and Electronic Commerce .....	1-1
Grow Your Online Business .....	1-2
MasterCard <i>SecureCode</i> Platform Components .....	1-3
Universal Cardholder Authentication Field and its Structure .....	1-3
Accountholder Authentication Value.....	1-4
Merchant Plug-In .....	1-4

## MasterCard and Electronic Commerce

Electronic commerce transactions account for a significant and increasing share of MasterCard® gross dollar volume. The number of remote transactions is increasing at a rapid rate annually. For this reason, it is important to position e-commerce and mobile commerce channels—Web access from PCs, PDAs, mobile phones, and other wireless-enabled devices—to increase gross dollar volume profitability by using security and authentication solutions that authenticate cardholders. This reduces chargebacks and expenses that are associated with disputed transactions.

From a risk perspective, the current MasterCard electronic and mobile transaction environment closely resembles traditional mail order/telephone order (MO/TO) transactions. The remote nature of these transactions increases risk, resulting in more cardholder disputes, and associated chargebacks.

These factors increase costs to all parties for managing disputes and chargebacks. More than 70 percent of all chargebacks for e-commerce transactions are associated with reason code 4837 (No Cardholder Authorization) or reason code 4863 (Cardholder Not Recognized). These reason codes are used where the consumer denies responsibility for the transaction and the acquirer lacks evidence of the cardholder's authentication, or the consumer does not recognize the transaction.

Proving that the cardholder conducted and authorized the transaction in a virtual, non-face-to-face environment of electronic and mobile commerce has been extremely difficult. The MasterCard® *SecureCode*™ program is designed to provide the infrastructure for an issuer security solution that reduces problems associated with disputed charges. Disputed charges affect all parties in a transaction, including the issuer, acquirer, cardholder, and merchant.

## Maestro and Electronic Commerce

Low credit card penetration in many countries has led to the use of inefficient payment forms like cash on delivery, check, and domestic transfer/ACH. MasterCard *SecureCode* will allow Maestro® cards to be used for Internet purchases in a safe and secure environment. MasterCard *SecureCode* allows Maestro to be the first fully authenticated global debit brand accepted on the Internet. Unless otherwise stated by domestic country rules, all Maestro Internet transactions are guaranteed. Please note that a merchant can not accept Maestro transactions unless they support MasterCard *SecureCode*.

## Grow Your Online Business

MasterCard *SecureCode* offers flexible, robust, and easy to implement solutions for cardholder authentication. Because requirements vary from issuer to issuer, MasterCard places a premium on flexibility, enabling issuers to choose from a broad array of security solutions for authenticating their cardholders. These solutions include password, smart card-based approaches, or other solutions of their own choosing. Issuers should decide on their authentication strategy by balancing their view of risk against the cardholder experience.

At launch of MasterCard *SecureCode* a “risk averse” strategy was visualized where every merchant transaction would be presented to the issuer for authentication and the issuer would ensure that the cardholder authenticated every transaction. As MasterCard *SecureCode* evolved, both retailers and issuers began practicing active risk management and now only those transactions deemed high-risk are authenticated. This risk-management is driving the adoption of dynamic solutions and resulting in a reduction in use of the initial static password solution.

MasterCard now formally supports this risk based approach for merchants. For additional information, and for information about Issuers through the Risk Based Authentication options, see, [Appendix F, MasterCard Advance Registration Program](#).

The most common of these cardholder authentication solutions for MasterCard and Maestro issuers has been the use of static or dynamic passwords. Dynamic password usage can be based on the Chip Authentication Protocol (CAP) that provides for the creation of a one-time use cardholder authentication password. This scenario is similar to what the cardholder experiences in the face-to-face environment using EMV chip card and personal identification number (PIN) and using the existing investments in EMV for new authentication purposes. This program provides a seamless integration of both EMV and 3-D Secure technologies that result in stronger authentication than traditional static password solutions. Currently, many new implementations take a risk-based approach to authentication and the use of dynamic codes, increasing both the strength of security while also improving the customer experience.

MasterCard *SecureCode* is the consumer-and-merchant-facing name for all existing and new MasterCard cardholder authentication solutions. While these solutions may each appear quite different on the surface, these various approaches converge around the Universal Card Authentication Field (UCAF™) mechanism and share a number of common features.

Two common features in all MasterCard cardholder authentication solutions include:

- MasterCard card or Maestro card cardholders are authenticated using a secure, unique, private code.
- The authentication data is transported from party-to-party via the MasterCard UCAF mechanism.

## MasterCard SecureCode Platform Components

The MasterCard *SecureCode* program platform is comprised of a number of layered components. As described in the following sections, each of the components provides for specific authorization and authentication functionality during the processing of a MasterCard *SecureCode* transaction. When combined, the platform provides a mechanism for online merchants to receive a similar global payment guarantee to one that brick-and-mortar retailers use with physical point-of-sale transactions.

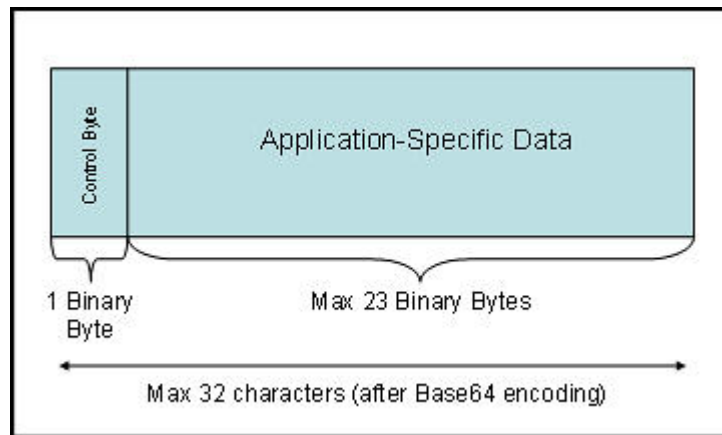
### Universal Cardholder Authentication Field and its Structure

UCAF is a standard, globally interoperable method of collecting cardholder authentication data at the point of interaction across all channels, including the Internet and mobile devices.

Within the MasterCard authorization networks (for example, MasterCard Worldwide Network, Single Message System, and RSC), UCAF is a universal, multi-purpose data transport infrastructure that is used to communicate authentication information among cardholder, issuer, merchant and acquirer communities. It is a variable length, 32-position field with a flexible data structure that can be tailored to support the needs of a variety of issuer security and authentication approaches.

The generic structure of UCAF is illustrated as follows:

**Figure 1.1—Universal Cardholder Authentication Field (UCAF) Structure**



The control byte contains a value that is specific to each security application. MasterCard is responsible for assigning and managing UCAF control byte values and the structure of UCAF application-specific data. Other solutions that use UCAF for authentication collection and transport will be assigned their own control byte value and the structure of the application-specific data will be tailored to support the specifics of the security protocol.

The current MasterCard *SecureCode* control byte definitions include:

Usage	Base64 Encoded Value	Hexadecimal Value
3-D Secure SPA AAV for first and subsequent transactions	J	x'8C'
3-D Secure SPA AAV for attempts	H	x'86'

In most UCAF implementations, the application-specific data is defined as binary data with a maximum length of 24 binary bytes including the control byte. However, there are some restrictions in the various MasterCard authorization networks regarding the passing of binary data in the authorization messages. As a result, all UCAF data generated by SPA algorithm-based MasterCard *SecureCode* implementations must be Base64 encoded at some point prior to being included in the authorization message. The purpose of this encoding is to produce a character representation that is approximately 33 percent larger than the binary equivalent. For this reason, the UCAF field is defined with a maximum length of 32 positions. For more information about Base64 coding, refer to [Appendix B, MasterCard \*SecureCode\* SPA Algorithm Specifications](#).

## Accountholder Authentication Value

The Accountholder Authentication Value (AAV) is a MasterCard *SecureCode* specific token that uses the UCAF field for transport within MasterCard authorization messages. It is generated by the issuer and presented to the merchant for placement in the authorization request upon successful authentication of the cardholder.

In the case of a chargeback or other potential dispute processing, the AAV will be used to identify the processing parameters associated with the transaction. Among other things, the field values will identify the:

- Issuer ACS that created the AAV.
- Sequence number that can be used to positively identify the transaction within the universe of transactions for that location
- Secret key used to create the Message Authentication Code (MAC), which is a cryptographic method that will not only ensure AAV data integrity but also bind the entire AAV structure to a specific PAN.

UCAF is the mechanism that is used to transmit the AAV from the merchant to issuer for authentication purposes during the authorization process.

## Merchant Plug-In

As part of the MasterCard *SecureCode* infrastructure requirements, all merchant endpoints must implement application software capable of processing 3-D Secure messages. An endpoint is described as any merchant or merchant processor platform, which directly connects to the MasterCard *SecureCode* infrastructure.

A merchant plug-in is a software application that is developed and tested to be compliant with the 3-D Secure protocol and interoperable with the MasterCard *SecureCode* infrastructure. The plug-in application is typically provided by a technology vendor and integrated with the merchant's commerce server. It serves as the controlling application for the processing of 3-D Secure messages.

**NOTE**

---

**If a retailer has qualified and accepted a merchant for the MasterCard Advance Registration Program (MARP), then MasterCard will assign a static AAV for use when the transaction is undertaken as MARP instead of standard SecureCode. This value is passed in plain text in the UCAF field. For additional information, see, [Appendix F, MasterCard Advance Registration Program](#).**

---

---

## Chapter 2 SecureCode 3-D Secure Solution

*This chapter provides a general overview of the MasterCard implementation of 3-D Secure for MasterCard® cards and Maestro® cards, including cardholder enrollment and payer authentication.*

---

Overview .....	2-1
Components.....	2-1
Issuer Domain.....	2-1
Cardholder Browser and Related Cardholder Software .....	2-1
Enrollment Server .....	2-2
Access Control Server .....	2-2
AAV Validation Server/Process.....	2-2
Acquirer Domain .....	2-2
Merchant Plug-In .....	2-2
Signature Validation Server .....	2-2
Interoperability Domain.....	2-3
Directory Server (DS).....	2-3
Certificate Authority .....	2-3
Transaction History Server .....	2-3
Attempts Server.....	2-3
Messages.....	2-4
Card Range Request/Response .....	2-4
Verification Request/Response.....	2-4
Payer Authentication Request/Response.....	2-4
Payer Authentication Transaction Request/Response .....	2-5
Cardholder Enrollment.....	2-5
Cardholder Enrollment Process.....	2-5
Sample Cardholder Enrollment Flow .....	2-6
Welcome .....	2-6
Terms and Conditions and Privacy Policy .....	2-7
Enter your Card Number .....	2-7
Verify Your Identity.....	2-8
Create Your MasterCard <i>SecureCode</i> .....	2-9
Congratulations.....	2-10
Cardholder Authentication.....	2-11
Sample Cardholder Authentication Process .....	2-11

Sample Cardholder Authentication Flow .....	2-13
Enter Payment Information .....	2-13
Confirm and Submit Order .....	2-13
Enter MasterCard <i>SecureCode</i> .....	2-13
Purchase Completed .....	2-14

## Overview

Cardholder authentication is the process of verifying cardholder account ownership during a purchase transaction in an online electronic commerce environment. All MasterCard® *SecureCode*™ solutions define and provide a base level of security around performing this authentication process. For this solution specifically, MasterCard is deploying its own implementation of 3-D Secure under the MasterCard *SecureCode* program branding for MasterCard® and Maestro®. This implementation of 3-D Secure includes support for the SPA algorithm and UCAF without any changes to the 3-D Secure specification, messages, or protocol.

The components described in this chapter are organized according to requirements that fall within the domains that are associated with the payment process.

These domains are associated with the payment process, and include:

- **Issuer Domain**—Systems and functions of the card issuing financial institutions and its customers.
  - Cardholder Browser
  - Related Cardholder Software
  - Enrollment Server
  - Access Control Server
  - AAV Validation Server/Process
- **Acquirer Domain**—Systems and functions of the acquirer and its customers.
  - Merchant Plug-In
  - Signature Validation Server
- **Interoperability Domain**—Systems, functions, and messages that allow the Issuer Domain and Acquirer Domain to interoperate. These components will be globally operated and managed by MasterCard.
  - Directory Server
  - Certificate Authority

## Components

Following is information about components related to the Issuer Domain, Acquirer Domain, and Interoperability Domain.

### Issuer Domain

Following is component information related to the Issuer Domain.

#### Cardholder Browser and Related Cardholder Software

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. Optional cardholder software to support implementations such as chip cards may also be included.

Both the browser and related software are considered to be off-the-shelf components that do not require any specific modification to support 3-D Secure.

### **Enrollment Server**

The purpose of the enrollment server is to facilitate the process of cardholder enrollment for an issuer's implementation of 3-D Secure under the MasterCard *SecureCode* program. The server will be used to perform initial cardholder authentication, as well as administrative activities such as MasterCard *SecureCode* resets and viewing 3-D Secure payment history. In some cases, the enrollment server and the access control server may be packaged together.

### **Access Control Server**

The access control server (ACS) serves two basic, yet vital, functions during the course of a MasterCard *SecureCode* online purchase. First, it will verify whether a given account number is enrolled in the MasterCard *SecureCode* program. Secondly, it will facilitate the actual cardholder authentication process.

### **AAV Validation Server/Process**

This server or process will be used to perform validation of the cardholder authentication data received by the issuer's authorization system in the authorization messages. MasterCard recommends that issuers validate the AAV contained in the authorization message prior to the authorization decision. This is considered a best practice, although not required.

## **Acquirer Domain**

Following is component information related to the Acquirer Domain.

### **Merchant Plug-In**

The merchant server plug-in creates and processes payer authentication messages and then returns control to the merchant software for further authorization processing. The plug-in is invoked after the cardholder finalizes the purchase request, which includes selecting the account number to be used, and submitting the order but prior to obtaining authorization for the purchase.

### **Signature Validation Server**

The signature validation server is used to validate the digital signature on purchase requests that have been successfully authenticated by the issuer. This server may be integrated with the merchant plug-in or may be a separately installed component.

## Interoperability Domain

Following is component information related to the Interoperability Domain.

### Directory Server (DS)

The MasterCard *SecureCode* global directory server provides centralized decision-making capabilities to merchants enrolled in the MasterCard *SecureCode* program. Based on the account number contained in the merchant enrollment verification request message, the directory will first determine whether the account number is part of a participating MasterCard or Maestro issuer's card range. It will then direct eligible requests to the appropriate issuer's access control server for further processing.

All implementations of this issuer platform **must** use the MasterCard *SecureCode* global directory server for processing MasterCard card and Maestro card transactions.

### Certificate Authority

The MasterCard Certificate Authority is used to generate and distribute all private hierarchy end-entity and subordinate certificates, as required, to the various components across all three domains.

These certificates include:

- MasterCard Root certificate (used for both MasterCard and Maestro)
- SSL Server and Client certificates issued under the MasterCard hierarchy
- Issuer Digital Signing certificates issued under the MasterCard hierarchy

In addition, SSL certificates based on a public root hierarchy are required. These certificates are not issued by the MasterCard Certificate Authority and must be obtained from another commercially available certificate-issuing provider. For additional information, see [Chapter 3, Component Certificate Requirements and Authentication Options](#).

### Transaction History Server

The Authentication History Server is a central repository of all authentication activity occurring within the issuer ACS for all transactions that occurred, including the PAREq and PAREs details . **The MasterCard *SecureCode* infrastructure does not currently support this component server, but may do so sometime in the future.**

### Attempts Server

**The MasterCard *SecureCode* infrastructure does not support this component server.**

## Messages

Following are message types associated with the 3-D Secure Solution process.

### Card Range Request/Response

**Message Pair: CRReq/CRRes**—For performance reasons, the Merchant Server Plug-In has the capability to cache the card ranges contained in the Directory, which indicate issuer participation in 3-D Secure. The Card Range Request/Response messages are used by the Merchant Server Plug-In as a way to request updates to the cache from the Directory. MasterCard discourages the use of caching and recommends that merchants check issuer participation against the directory server, in real time for each transaction.

---

#### NOTE

**Any merchant that wants to use caching must apply to do so, which will require testing and, if accepted, compliance with procedures distributed to all merchants accepted for caching.**

---

### Verification Request/Response

**Message Pair: VReq/VERes**—The first step in the payer authentication process is to validate that the cardholder account number is part of an issuer's card range, which is participating in 3-D Secure. The Verification Request/Response messages are sent from the Merchant Server Plug-In to the Directory to check card range eligibility. If the specified account number is contained within a MasterCard *SecureCode* eligible card range, this message is then sent from the Directory to the Access Control Server to check if the specific account number is enrolled and active to participate in 3-D Secure.

For those merchants that cache the contents of the MasterCard *SecureCode* directory server, this message is not used if the cache indicates that the issuer is not enrolled in 3-D Secure. If the cache does indicate that the issuer is enrolled, or if no cache is being maintained, this message must be formatted and processed as described.

### Payer Authentication Request/Response

**Message Pair: PReq/PARes**

After determining that a cardholder is enrolled to participate in 3-D Secure, the actual process of payer authentication is performed for each online purchase. The Payer Authentication Request/Response messages are sent from the Merchant Server Plug-In to the Access Control Server to initiate the actual authentication. At this point, the cardholder will be presented with an authentication window and asked to enter their MasterCard *SecureCode*.

The Access Control Server will perform authentication and, if successful, will generate an Accountholder Authentication Value (AAV). It is returned to the merchant within the PAREs message. For successfully authenticated transactions, this AAV must be sent by the merchant to the acquirer and forwarded to the issuer as part of the authorization request.

## Payer Authentication Transaction Request/Response

**Message Pair: PATransReq/PATransRes**—Following authentication, it may be desirable to centralize storage of authentication requests for later dispute processing. The Payer Authentication Transaction Request/Response messages provide a record of this authentication activity sent from the ACS to the History Server.

---

### NOTE

**The MasterCard *SecureCode* global infrastructure does not support these messages now, but may sometime in the future.**

---

## Cardholder Enrollment

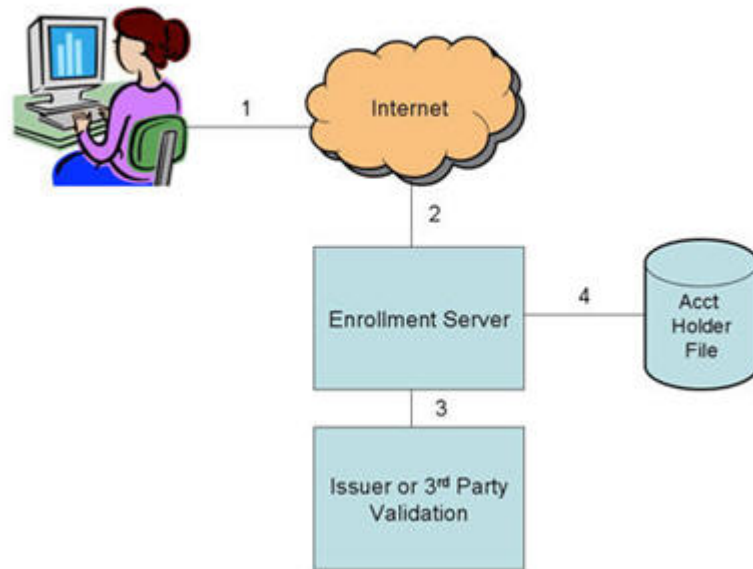
The following paragraphs outline the cardholder enrollment process for MasterCard *SecureCode*.

### Cardholder Enrollment Process

Enrollment is the process whereby authorized MasterCard and Maestro branded cardholders will activate their cards for a specific issuer's MasterCard *SecureCode* program. Part of the planning process for building a 3-D Secure infrastructure will involve determining exactly how this process will work.

The major component associated with enrollment is the enrollment server. It is responsible for driving the process under which the cardholder:

- Validates that their account number is designated as eligible to participate in MasterCard *SecureCode* by the card issuing financial institution.
- Is authenticated by the card issuing financial institution through the validation of secret questions, independently determined by each issuer participating in the program.
- Sets up and defines their MasterCard *SecureCode*.
- Performs functions such as profile administration (including MasterCard *SecureCode* and e-mail changes) and review of recent purchases.



Typically, the following steps are necessary to authenticate the cardholder:

Step	Description
1.	The cardholder visits an issuer enrollment site. This may be accessible, for example, from the issuer's Web site or home banking system.
2.	The cardholder is asked to provide issuer identified enrollment data. During this phase of the process, the cardholder is asked a series of secret questions to prove identity to the issuer.
3.	The enrollment data, or answers to the secret questions, is validated by the issuer.
4.	If the appropriate answers are provided, the cardholder is considered to be authenticated and is allowed to establish his or her MasterCard <i>SecureCode</i> to be associated with the specified account number. The MasterCard <i>SecureCode</i> is stored by the issuer for later use during online purchases at participating merchants.

## Sample Cardholder Enrollment Flow

The following sample cardholder enrollment flow is identical for both MasterCard and Maestro cardholders. Contact your Maestro e-commerce representative for Maestro branded sample screens.

### Welcome

The welcome screen introduces cardholders to the benefits of MasterCard *SecureCode*.

Figure 2.1—Cardholder Welcome Page



## Terms and Conditions and Privacy Policy

Prior to cardholder authentication, any issuer-specific terms and conditions statement, along with a privacy policy, will be presented to cardholders for acceptance. Acceptance of this information may be a requirement for the process flow to continue.

## Enter your Card Number

Cardholders will be prompted to enter their card number. This will be used to perform a check to validate that the card number is part of a MasterCard or Maestro issuer card range, which is participating in the MasterCard *SecureCode* program.

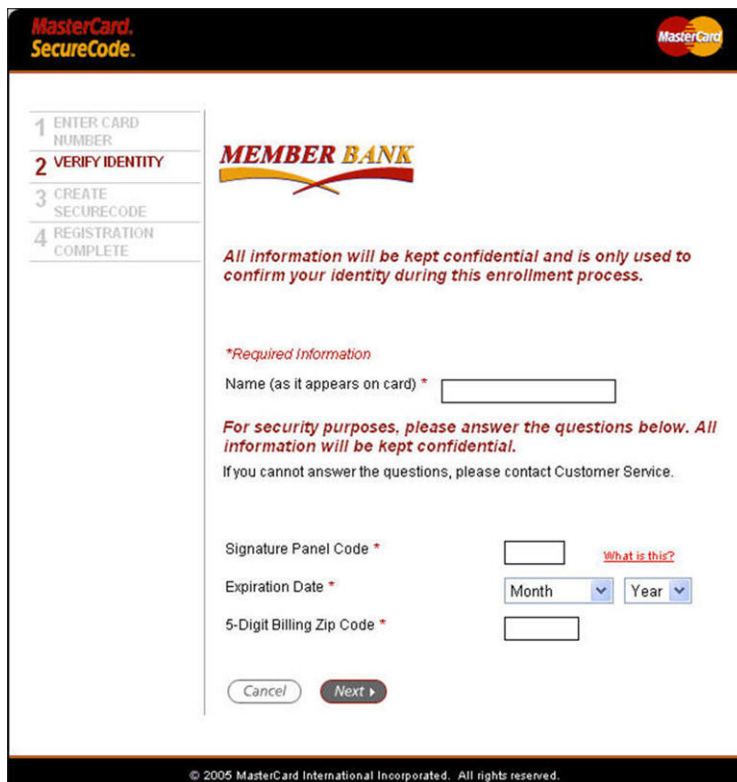
Figure 2.2—Cardholder Provides Card Number

The screenshot shows the MasterCard SecureCode Member Bank enrollment interface. At the top left, it says "MasterCard, SecureCode." and at the top right is the MasterCard logo. On the left side, there is a vertical progress bar with four steps: 1 ENTER CARD NUMBER (highlighted), 2 VERIFY IDENTITY, 3 CREATE SECURECODE, and 4 REGISTRATION COMPLETE. The main content area features the "MEMBER BANK" logo and the text: "It's free, quick.... and secure! Enter your information below to confirm your identity. This information will be transmitted securely and will enable you to create your SecureCode™. This information will not be shared with anyone." Below this is a section titled "\*Required Information" with two input fields: "Card Number\*" and "Email Address". The Card Number field has a note: "Please do not include spaces or hyphens." The Email Address field has a link: "How will my email be used?". At the bottom of the form are "Cancel" and "Next >" buttons. The footer contains the copyright notice: "© 2005 MasterCard International Incorporated. All rights reserved."

## Verify Your Identity

This is the first of two displays that may be used to collect cardholder authentication data. The “Name (as it appears on card)” field allows for MasterCard *SecureCode* registration of multiple individuals using the same account number (for example, husband and wife).

Only the Name and Expiration Date fields are required. All additional fields are customizable as determined by the issuer.



MasterCard.  
SecureCode.

1 ENTER CARD NUMBER  
2 VERIFY IDENTITY  
3 CREATE SECURECODE  
4 REGISTRATION COMPLETE

**MEMBER BANK**

All information will be kept confidential and is only used to confirm your identity during this enrollment process.

*\*Required Information*

Name (as it appears on card) \*

For security purposes, please answer the questions below. All information will be kept confidential.  
If you cannot answer the questions, please contact Customer Service.

Signature Panel Code \* [What is this?](#)

Expiration Date \* Month Year

5-Digit Billing Zip Code \*

Cancel Next >

© 2005 MasterCard International Incorporated. All rights reserved.

A second screen can be used to collect cardholder authentication data. All questions on this screen are customizable, as determined by the issuer.

## Create Your MasterCard SecureCode

Assuming that all cardholder data is successfully validated, the cardholder will now have the opportunity to create:

1. An individual MasterCard *SecureCode* to use when paying with the designated MasterCard card or Maestro card at participating merchants.
2. A secret question and corresponding answer that can be used in case of a forgotten MasterCard *SecureCode*. Another option, used extensively by many implementations, is to ask cardholders the original authentication questions again.
3. A Personal Greeting. This greeting will be displayed on the authentication window every time a purchase is made. The presence of this field on the authentication window is an assurance to the cardholder that he or she is communicating with his or her issuing financial institution.

**MasterCard. SecureCode.**

1 ENTER CARD NUMBER  
2 VERIFY IDENTITY  
**3 CREATE SECURECODE**  
4 REGISTRATION COMPLETE

**MEMBER BANK**

**Create Your SecureCode™**

This is the secret code you'll be asked to enter at participating merchant websites during check-out.

*\*Required Information*

SecureCode\*   
6-10 characters and at least 1 letter and 1 number.

Confirm SecureCode\*

This cardholder verification request screen will appear automatically when you check-out at participating merchants.

**Your Bank** **MasterCard. SecureCode.**

**Enter Your SecureCode™**

Please enter your MasterCard SecureCode in the field below to confirm your identity for this purchase. This information is not shared with the merchant.

Merchant: Sample SDK Implementation  
Amount: **33.99 USD**  
Date: 25.08.06  
Card number: XXXX XXXX XXXX 0426  
Personal Greeting: Welcome MC  
SecureCode:

[Forgot your SecureCode?](#)

© 2006 MasterCard International Incorporated. All rights reserved.

**Create your Personal Greeting**

This personal greeting will be displayed whenever your SecureCode is requested by your bank. It's your assurance that the request coming from your bank is valid.

Create Personal Greeting\*   
1-30 characters -- must differ from your SecureCode.

If you forget your SecureCode you can always return to this site to re-register.

© 2005 MasterCard International Incorporated. All rights reserved.

## Congratulations

The cardholder is now ready to start shopping!

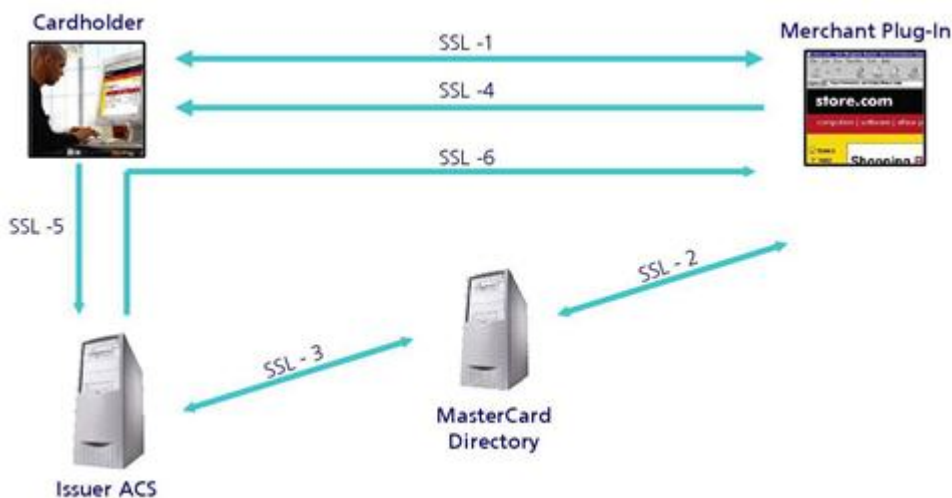


## Cardholder Authentication

Following is information about the cardholder authentication process.

### Sample Cardholder Authentication Process

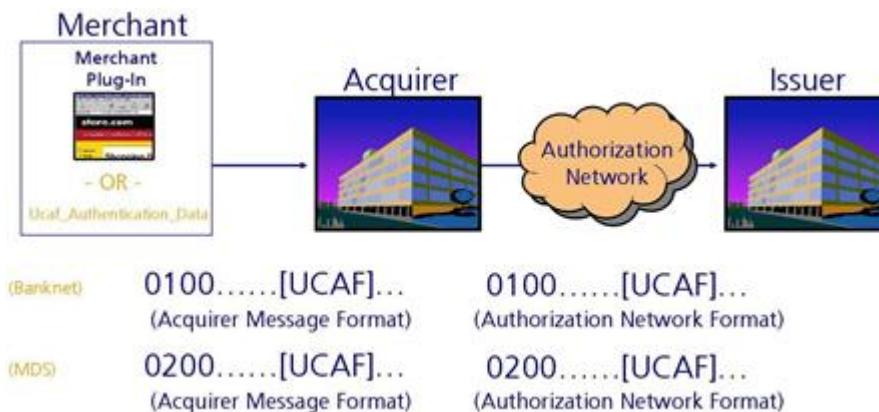
The sample flow that follows assumes that the cardholder has already enrolled in his or her issuer's MasterCard *SecureCode* program and obtained a MasterCard *SecureCode* to use while shopping online at participating merchants.



The figure above also assumes that all communication channels between the various components are properly secured using the Secure Socket Layer (SSL) protocol.

<b>Link</b>	<b>Description</b>
SSL-1	The cardholder shops at the merchant and, when ready to checkout, enters the appropriate payment information—including the account number.
SSL-2	The Merchant Plug-In queries the Directory to verify the enrollment status for a specific issuer using the verification request messages. It is possible that this step will be performed locally at the merchant via the local MasterCard directory cache, if applicable.
SSL-3	If the directory indicates that an issuer is participating, then the directory must forward a request to the issuer's Access Control Server to check the enrollment status of a specific cardholder. The configuration information in the Directory will indicate exactly which Access Control Server will perform the check. The resulting response will flow back over the same links to the Merchant Plug-In.
SSL-4	If the Access Control Server indicates that a specific cardholder is participating, the Merchant Plug-In creates the Payer Authentication Request message and sends it to the cardholder's browser.
SSL-5	The cardholder browser redirects the message to the appropriate Access Control Server to perform cardholder authentication. When the Access Control Server receives the Payer Authentication Request message, it causes the user authentication dialog to begin. This in turn causes a separate authentication window to appear to the cardholder that will facilitate the cardholder authentication process.
SSL-6	The Access Control Server authenticates the cardholder MasterCard <i>SecureCode</i> , constructs the SPA AAV for the MasterCard implementation of 3-D Secure, and builds and digitally signs the Payer Authentication Response message. It is returned to the Merchant Plug-In, at which point the cardholder authentication window will disappear.

Once cardholder authentication has been completed, the merchant is required to pass the corresponding SPA AAV to the acquirer via the UCAF field within the authorization message. This value is then passed from the acquirer to the issuer as part of the authorization message.



When received by the issuer, the AAV can be validated as part of authorization request processing, as well as archived for use in potential cardholder disputes.

## Sample Cardholder Authentication Flow

The following sample cardholder authentication flow is identical for both MasterCard and Maestro cardholders.

### Enter Payment Information

The cardholder will shop at a merchant location just as they would today. After selecting the items to be placed into the shopping cart, the payment card information to be used for the transaction is entered.

### Confirm and Submit Order

Once all of the payment and shipping information has been entered, the cardholder is typically given an opportunity to review the purchase one last time before submitting the order.

### Enter MasterCard *SecureCode*

Upon submitting the final order, the cardholder will be presented with an authentication window from their MasterCard card or Maestro card-issuing bank. At this point, the cardholder will enter his or her MasterCard *SecureCode* value to perform authentication processing.

The screenshot shows a web-based authentication window. At the top left is the 'MEMBER BANK' logo, and at the top right is the 'MasterCard SecureCode' logo. The main heading is 'Enter Your SecureCode™'. Below this, a message asks the user to enter their SecureCode to confirm their identity. A list of transaction details is provided: Merchant (MasterCard Store), Amount (199.99 USD), Date (12:09:10), Card number (XXXX XXXX XXXX 3206), and Personal Greeting (Hello). The SecureCode field is empty with a red underline. A link for 'Forgot your SecureCode?' is below the field. At the bottom right, there are 'Submit', 'Help', and 'Cancel' buttons.

Merchant:	MasterCard Store
Amount:	199.99 USD
Date:	12:09:10
Card number:	XXXX XXXX XXXX 3206
Personal Greeting:	Hello
SecureCode:	<input type="text"/>

[Forgot your SecureCode?](#)

## Purchase Completed

After validation of the cardholder MasterCard *SecureCode* by the issuing bank, the authentication window will disappear and the authorization of the payment card will complete as usual.

---

## Chapter 3 Component Certificate Requirements and Authentication Options

*This chapter provides a general overview of the certificate requirements and component authentication options available for implementation.*

---

Overview .....	3-1
Functional Certificate Authority Hierarchy .....	3-1
Public Zone .....	3-2
Trusted Zone .....	3-2
Configuration Options .....	3-2
Operational Certificate Authority Hierarchy .....	3-3
Certificates .....	3-4
Root Certificate .....	3-4
Issuer Directory Subordinate Certificate.....	3-4
ACS Digital Signing Certificate .....	3-4
Issuer ACS Server Certificate.....	3-5
Directory ACS SSL Client Certificate.....	3-5
Merchant MPI SSL Client Certificate.....	3-5
Requesting Certificates.....	3-6

## Overview

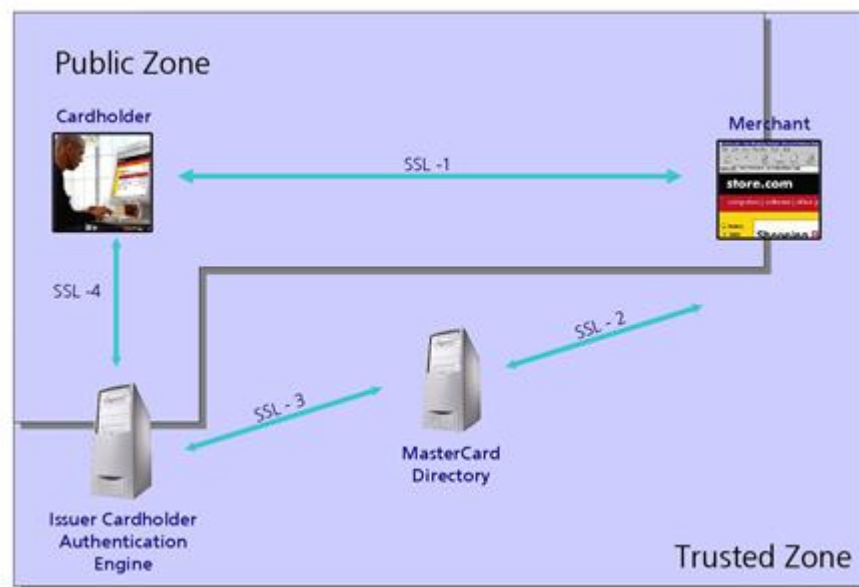
All components within a MasterCard® *SecureCode*™ infrastructure are required to provide appropriate transport security to the data being passed between them.

This is accomplished by using the Secure Socket Layer (SSL) protocol, which provides for the following:

- **SSL Server Certificate Authentication**—This provides a mechanism for the client, for example, the party requesting the communication session, to assure that the server sending the data is a trusted party.
- **SSL Client Certificate Authentication**—This is similar to the server certificate authentication except that it also allows the server to assure that the client requesting the data is a trusted party. Failure of the SSL certificates to authenticate will result in a failure of the communication session to establish.

## Functional Certificate Authority Hierarchy

From a functional viewpoint, all certificates used by MasterCard *SecureCode* solutions will be issued under either a public hierarchy maintained by a commercial entity or under the MasterCard private hierarchy.



## Public Zone

The inclusion of a transaction flow in the public zone is a direct result of the requirement for a secure communication channel with the cardholder's browser. Because it is unrealistic to require cardholders to import a MasterCard root certificate to participate in the protocol, all communication channels within this zone **must** use SSL certificates that are created from a public root hierarchy. The communication channels within this zone will be secured with SSL server certificates only. The cardholder will not be required to have a SSL client certificate.

MasterCard recommends that all communications within this zone be based on 128-bit encryption ciphers.

The following table highlights the communication links, which fall within the public zone.

MasterCard <i>SecureCode</i> Platform	SSL-1	SSL-2	SSL-3	SSL-4
3-D Secure with SPA AAV	Yes	No	No	Yes

## Trusted Zone

The inclusion of a transaction flow in the trusted zone is a direct result of the requirement of a more trusted, secure communication channel between a finite set of participants. As a result, this zone will contain all non-cardholder communication channels.

The following table highlights the communication links for each MasterCard *SecureCode* platform, which fall within the private zone.

MasterCard <i>SecureCode</i> Platform	SSL-1	SSL-2	SSL-3	SSL-4
3-D Secure with SPA AAV	No	Yes	Yes	No

## Configuration Options

The 3-D Secure with SPA AAV issuer platform has the following configuration requirements within the private zone:

### SSL-2 link:

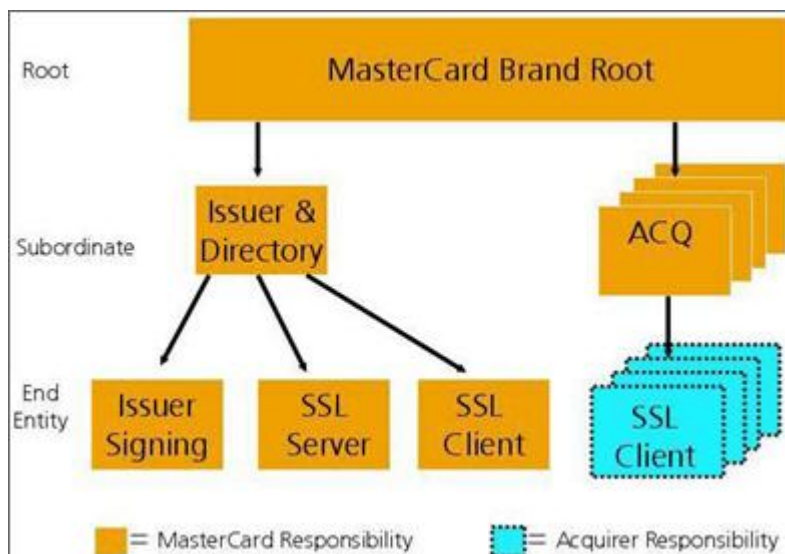
- The merchant plug-in must use a SSL client certificate based on the MasterCard private hierarchy. If a processor is using the merchant plug-in, MasterCard does not require an individual certificate for each merchant. However, the processor will be required to use a separate and distinct client certificate for each applicable acquirer.
- The Directory will require an SSL server certificate based on a public hierarchy. At the time of publication, the root is a VeriSign® certificate.

**SSL-3 link:**

- The Directory will use an SSL client certificate based on a MasterCard private hierarchy.
- The ACS must use an SSL server certificate based on a MasterCard private hierarchy. In order for this to provide the proper level of security, the following configuration issues must be addressed:
  - The URL for connectivity with the Directory must be different than the one used for connectivity with the cardholder.
  - The Directory URL must be configured to accept only certificates based on the MasterCard root certificate. Failure to present a proper certificate from the MasterCard hierarchy must result in a failed session attempt.

## Operational Certificate Authority Hierarchy

The MasterCard certificate authority will be used to issue specific MasterCard private hierarchy end-entity and subordinate certificates only. All public rooted certificates used by the MasterCard *SecureCode* issuer platforms must be obtained from commercially available sources.



The following table indicates responsibility for creating, signing, and managing the various roots, subordinates, and end entity certificates in the hierarchy.

Certificate	Creation	Signing	Maintenance
MasterCard Root	MasterCard	MasterCard	MasterCard
Issuer/Directory Subordinate	MasterCard	MasterCard	MasterCard
Acquirer Subordinate	MasterCard	MasterCard	Acquirer
Issuer/Directory Signing End-Entity	MasterCard	MasterCard	MasterCard

<b>Certificate</b>	<b>Creation</b>	<b>Signing</b>	<b>Maintenance</b>
Issuer/Directory SSL Server End-Entity	MasterCard	MasterCard	MasterCard
Issuer/Directory SSL Client End-Entity	MasterCard	MasterCard	MasterCard
Acquirer SSL Client End-Entity	Acquirer	Acquirer	Acquirer

## **Certificates**

Following is information about different types of certificates.

### **Root Certificate**

The MasterCard CA has created the root certificate specifically for MasterCard *SecureCode*. The root certificate is self-signed and is shared by MasterCard and Maestro.

Validity Period: 10 Years

Key Size: 2048 bits

### **Issuer Directory Subordinate Certificate**

This subordinate certificate has been created by the MasterCard CA and signed by the MasterCard root. The subordinate certificate is used to sign all end-entity certificates used for communication between the MasterCard Directory and issuer access control servers.

Validity Period: Through the validity of the root

Key Size: 2048 bits

### **ACS Digital Signing Certificate**

This end-entity certificate, based on certificate requests received from issuer access control server implementations, will be created by the MasterCard CA and signed by the Issuer/Directory subordinate certificate. The ACS digital signing certificate is used by the issuer's access control server to digitally sign all payer authentication response messages returned to the merchant.

Validity Period:	4 Years
Key Usage Period	3 Years The difference between the validity and key usage periods is a direct result of having to perform authentications on transactions after the key usage period has expired.
Key Size:	1024 bits

### **Issuer ACS Server Certificate**

This end-entity certificate, based on certificate requests received from issuer access control server implementations, will be created by the MasterCard CA and signed by the Issuer/Directory subordinate certificate. These certificates are used by the issuer access control server to establish SSL communications with the MasterCard Directory server.

Validity Period:	Through the validity of the root and associated subordinate
Key Size:	Recommended—2048 bits Minimum—1024 bits

### **Directory ACS SSL Client Certificate**

This end-entity certificate will be created by the MasterCard CA and signed by the Issuer/Directory subordinate certificate. These certificates are used by the MasterCard Directory server to establish SSL communications with issuer access control server implementations.

Validity Period:	Through the validity of the root and associated subordinate
Key Size:	Recommended—2048 bits Minimum—1024 bits

### **Merchant MPI SSL Client Certificate**

This end-entity certificate will be created by the MasterCard CA and signed by the Acquirer subordinate certificate. These certificates will be used by the merchant components to establish SSL client communication using the MasterCard private hierarchy.

## Component Certificate Requirements and Authentication Options

### Operational Certificate Authority Hierarchy

---

Validity Period:	May be up through the expiration date of the Root and Acquirer subordinate CA certificates.
Key Usage Period	Recommended—2048 bits Minimum—1024 bits The difference between the validity and key usage periods is a direct result of having to perform authentications on transactions after the key usage period has expired.
Common Name (CN):	The common name must be populated with one of the following characteristics of the site that will use the certificate: <ul style="list-style-type: none"><li>• Domain Name (For example, www.merchant.com)</li><li>• Externally visible IP address (For example, 1.2.3.4)</li><li>• Externally visible IP address range (For example, 1.2.3.0-1.2.3.255)</li></ul>
Organizational Unit (OU)	Name of the merchant or merchant processor (if applicable) requesting the certificate Acquirer BIN, as indicated in the associated acquirer enrollment forms, and Name of the acquirer. The two fields must be separated by a colon, for example, 543210:Acquirer Name
Country	Country where the merchant or merchant processor is located. This should be the ISO 3166 2 character country code (for example, US)

## Requesting Certificates

For more information about the certificate request process, refer to the *MasterCard SecureCode Production Procedures* publication, which is available by request sent to the following e-mail address: [securecode@mastercard.com](mailto:securecode@mastercard.com). All requests that fail to follow the published procedures will be rejected.

---

## Chapter 4 Merchants

*This chapter provides a general overview of the various activities and requirements associated with building and maintaining the merchant components required to support MasterCard® SecureCode™.*

---

Overview .....	4-1
General Responsibilities.....	4-1
Infrastructure.....	4-1
Establishment of MasterCard <i>SecureCode</i> Operating Environment.....	4-2
Authorization System Enhancements .....	4-2
Passing the AAV in the Authorization Message.....	4-2
AAV Usage .....	4-3
Passing the Electronic Commerce Indicator in the Authorization Message.....	4-3
Recurring Payments .....	4-4
Maestro Considerations.....	4-5
Required use of SecureCode.....	4-5
Account Number Length Requirements .....	4-5
CVC2 and Maestro .....	4-5
Maestro Acceptance Rules .....	4-5
Additional Maestro Propositions and Considerations in E-commerce when using SecureCode.....	4-5
Customization .....	4-5
Program Identifier Usage Guidelines .....	4-5
Integrated Support for Merchant Plug-In Processing .....	4-6
Consumer Message on Payment Page .....	4-8
Creation of Cardholder Authentication Window.....	4-8
Pop-Up Authentication Windows .....	4-8
Inline Windows .....	4-8
With Frames.....	4-8
Without Frames.....	4-9
TERMURL Field.....	4-9
Replay Detection .....	4-9
Merchant Server Plug-In Configuration.....	4-10
Initialization of MasterCard Directory URL.....	4-10
Initialization of MPI Processing Timers.....	4-10
Cache Expiration Timers.....	4-10
Transaction Time-out Timers .....	4-10

## Merchants

---

Initialization of MPI Processing Parameters .....	4-11
TERMURL.....	4-11
Zero or Empty Parameters .....	4-11
Operational.....	4-12
Loading of MasterCard Root Certificates .....	4-12
Loading of MasterCard SSL Client Certificate .....	4-12
MPI Log Monitoring.....	4-12
MPI Authentication Request/Response Archival .....	4-12
Accountholder Authentication Value (AAV) Processing .....	4-13
Identification of SPA AAV Format in PAREs.....	4-13
Validation of Payer Authentication Response (PAREs) Signature .....	4-13
Global Infrastructure Testing Requirements.....	4-13
MasterCard Site Data Protection Program .....	4-13
Merchant Processing Matrix .....	4-14
Formatted File Type.....	4-14

## Overview

This chapter outlines the major activities and requirements for building and maintaining the merchant components that are required to support MasterCard® *SecureCode*™.

The activities and requirements will be separated into five primary categories:

Category	Description
Infrastructure	Requirements related to installation of new hardware and software components.
Customization	Requirements related to customizing or configuring vendor products.
Operational	Requirements related to operating the components in a production environment, including any process oriented changes that may be required.
Accountholder Authentication Value (AAV) Processing	Requirements related to handling and processing of the AAV.
Global Infrastructure Testing Requirements	Requirements related to testing of MasterCard <i>SecureCode</i> platform components.

### DEFINITION

**Throughout this chapter, there are references to a merchant endpoint. This is the entity that is actually operating the Merchant Plug-In software. These may include, for example, individual merchants, hosting providers, and payment service providers. Not all merchants participating in the MasterCard *SecureCode* program are considered endpoints.**

## General Responsibilities

MasterCard requires all merchants to ensure that MasterCard *SecureCode* is not the only fraud management tool used to manage fraud. Additional options available within standard card processing such as CVC2, and Address Verification Service (AVS) (available in some territories) should also be used. Many suppliers now offer fraud monitoring systems that take other non-card information available for capture during the e-commerce shopping experience. Check with your acquirer or shopping cart/MPI vendor for options. If using a Service Provider to supply the checkout and MasterCard *SecureCode* experience, additional options are likely available.

## Infrastructure

Following are the merchant infrastructure requirements for the installation of new hardware and software components that support MasterCard *SecureCode*.

## Establishment of MasterCard *SecureCode* Operating Environment

All merchants participating in the MasterCard *SecureCode* program are required to install or have access to a 3-D Secure v 1.0.2 or higher compliant Merchant Server Plug-In. A current list of vendors compliant with MasterCard *SecureCode* is located at: [www.mastercardmerchant.com/securecode/vendors.html](http://www.mastercardmerchant.com/securecode/vendors.html).

## Authorization System Enhancements

Following are enhancements to the authorization system for supporting MasterCard *SecureCode*.

### Passing the AAV in the Authorization Message

MasterCard requires that the SPA AAV returned to the merchant in the Payer Authentication Response (PAREs) message be included in all successfully cardholder authenticated e-commerce transactions. Currently, this is defined as being when the merchant plug-in detects a value of “Y” in the transaction status field of the PAREs message.

---

#### NOTE

**MasterCard currently uses a transaction status of “A” only when the cardholder opts out of enrollment during activation during shopping (ADS). For authorizations covered by the merchant-only liability shift, these transactions still meet the liability shift qualifying criteria when authorized by the issuer. Refer to the [Merchant Processing Matrix](#) for details of when to pass AAV and liability shift provided.**

---

Merchants must ensure that they follow the message formatting requirements of their acquirer when generating UCAF related authorization requests.

There are two potential issues to consider:

1. MasterCard requires that the SPA AAV contained in the authorization from the acquirer to the issuer be Base64 encoded. Passing this data in binary format is not an option. Merchant plug-in software typically provides the SPA AAV returned in the PAREs message already in this format. While some acquirers allow merchants to simply pass the Base64 encoded SPA AAV through in the authorization, others have varying requirements.

Depending on the specific merchant system and acquirer message formats, it may be necessary for the SPA AAV to be converted between ASCII and EBCDIC encoding prior to it being sent to the acquirer. Any such conversion must only be performed on the SPA AAV **after** it has been Base64 encoded. Any attempt to modify the binary representation of the SPA AAV will result in corruption of the data and the inability of the issuer to perform cardholder authentication verification processing.

The only exception to the Base 64 encoding requirement of an AAV is when MasterCard supplies this AAV to the merchant as a static code for use in MARP transactions. This static AAV must be passed in plain text. For additional information on MARP, see Appendix D, [MasterCard Advance Registration Program](#).

For more information about Base64 encoding, refer to [Appendix B, MasterCard SecureCode SPA Algorithm Specifications](#).

2. While an authentication status of “A” is a valid PAREs status response and will contain a SPA AAV, it is not considered to be a successful cardholder authentication. The AAV resulting from such a transaction is identified by a lower case “h” in the first position (Base64 encoded). Acquirers must ensure that transactions with a PAREs status of “A” are sent to MasterCard as merchant only transactions. This is similar to what would happen in the case of a status of “N” in the VERes message. **In these cases, MasterCard requires that the SPA AAV provided with the PAREs message be excluded from the authorization message.** In some cases, the merchant will be required to exclude this from the authorization message sent to their acquirer. In other cases, the acquirer may require that the merchant send the SPA AAV and then the acquirer will exclude it prior to sending the authorization message to MasterCard.

If questions arise, merchants should consult with their acquirers for more detailed information. Refer to the [Merchant Processing Matrix](#) for additional information.

## AAV Usage

The AAV contained within a single authorization request must match the AAV value returned by the issuer for a single associated authentication request. Therefore, an AAV can be used only once in a single authorization message and must not be stored for reuse after receiving authorization.

## Passing the Electronic Commerce Indicator in the Authorization Message

An electronic commerce indicator (ECI) flag will be present in a PAREs message when the status field contains a value of “Y” or “A.” The 3-D Secure protocol defines that this ECI field be determined by each brand. As a result, MasterCard has adopted values that may be different from other participating payment brands. When these values are used within the MasterCard authorization and clearing systems, they are referred to as Security Level Indicators (SLIs).

Most, if not all, acquirers and payment processors have defined the ECI as a required field in their authorization request message formats. Each merchant must ensure that the MasterCard ECI value is properly translated to a valid value as defined in the appropriate acquirer or payment processor authorization message format. Failure to perform the appropriate translation may affect the ability to obtain successful authorizations.

MasterCard has currently defined two ECI values. The following table indicates the relationship between these values and the status field in the PAREs message. Any questions on translating MasterCard defined values for authorization should be directed to your acquirer or payment processor.

PAREs Status Field	Description	MasterCard ECI Value
Y	Cardholder was successfully authenticated	02
A	Authentication could not be completed but a proof of authentication attempt was provided. The presence of the AAV from this response in a corresponding authorization message does not constitute a fully authenticated transaction and does not qualify for chargeback protection under the global liability shift as outlined in <a href="#">Chapter 1, Overview</a> .  For more information, please refer to <a href="#">Appendix B, MasterCard SecureCode SPA Algorithm Specifications</a> .	01
N	Cardholder authentication failed.	Absent
U	Authentication could not be completed because of technical or other problems.	Absent

**NOTE**

MasterCard has additional definitions of SLIs that are not generated by the PAREs received but that may need to be used by the merchant. Refer to the [Merchant Processing Matrix](#) section for additional information on SLIs.

---

## Recurring Payments

Only the initial authorization request for a recurring payment may be e-commerce transactions and may contain UCAF data. Merchants must not provide UCAF data in any subsequent recurring payment authorizations as these are not considered electronic commerce transactions by MasterCard and are not eligible for participation in the MasterCard *SecureCode* program.

With the following exception, Maestro® cards are not eligible to be used for recurring payments.

**Effective 1 April 2011, recurring payments on Maestro cards issued in the Europe region are valid but subject to specific acceptance rules.** Refer to the *Maestro Global Rules* for additional information about Maestro.

## Maestro Considerations

The following requirements and activities are specific to merchant support of Maestro cards as part of the MasterCard *SecureCode* program. Contact your acquirer for a complete set of Maestro e-commerce acceptance requirements.

### Required use of SecureCode

Maestro rules require that all e-commerce merchants accepting Maestro cards must use MasterCard *SecureCode* for all transactions, or apply and be accepted for entry to MARP. See [Appendix F, MasterCard Advance Registration Program](#) for additional information.

### Account Number Length Requirements

Maestro merchants must support cardholder account numbers that are 13–19 digits in length.

### CVC2 and Maestro

Merchants should be aware that not every Maestro card in issuance has a CVC2 and this should be factored in during checkout design.

### Maestro Acceptance Rules

For additional information about accepting Maestro in e-commerce and the rules pertaining to Maestro Acceptance refer to the *Maestro Global Rules*.

### Additional Maestro Propositions and Considerations in E-commerce when using SecureCode

For additional information, refer to [Appendix D, Maestro Considerations](#).

## Customization

Following are merchant requirements for customizing or configuring vendor products in support of MasterCard *SecureCode*.

### Program Identifier Usage Guidelines

Merchants are required to adhere to the applicable usage guidelines as outlined at [www.mastercard.com/us/merchant/solutions/mastercard\\_securecode.html](http://www.mastercard.com/us/merchant/solutions/mastercard_securecode.html). Proof of adherence must be provided to MasterCard as a condition of successful completion of SecureCode functional testing. MasterCard recommends that all screenshots be provided for review as soon as possible in case changes are required.

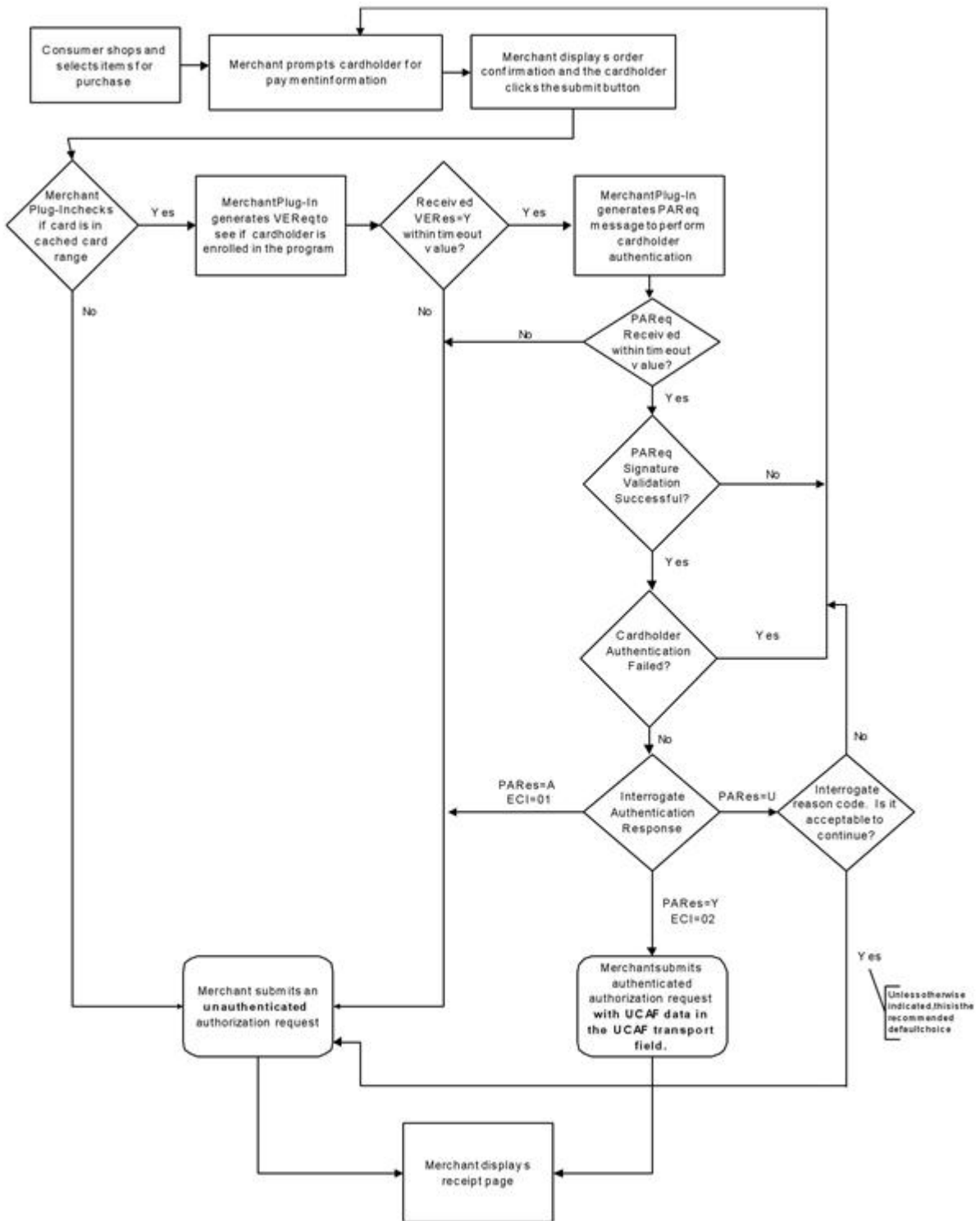
A copy of the MasterCard *SecureCode* logo artwork, as well as any updates to the program identifier usage guidelines, is available for download at [www.mastercardbrandcenter.com/us/getourbrand/index.shtml](http://www.mastercardbrandcenter.com/us/getourbrand/index.shtml).

## **Integrated Support for Merchant Plug-In Processing**

The following diagram depicts a sample high-level flow of a transaction through a merchant's e-commerce site that has integrated support for MasterCard *SecureCode*.

The following figure indicates merchant best practices regarding MasterCard *SecureCode* processing.

Figure 4.1—Sample Integrated MasterCard SecureCode Solution



At the completion of the authentication process, the merchant should create an authorization message, which contains the appropriate UCAF-related data fields. The associated merchant acquirer or processor will provide message specifications detailing UCAF-related data fields within their authorization, clearing and settlement records.

## Consumer Message on Payment Page

MasterCard recommends the use of a consumer message on the payment page to further indicate merchant participation in the program.

## Creation of Cardholder Authentication Window

The 3-D Secure protocol is designed so that the creation of the cardholder authentication window is performed by the merchant. The actual content of the window is controlled by the cardholder's issuing financial institution. There are two primary methods for creation of this window, however only one approach, inline windows, is now acceptable for deployment. Existing merchants are expected to convert to an inline window implementation.

---

### NOTE

**Previous implementation approaches based on pop-up authentication windows are no longer supported for new merchant implementations. As the requirement to cease using pop-up windows has been in place since 2005, any merchant that is found to support a pop-up window will be deemed as out of compliance with MasterCard *SecureCode* and may have their facility terminated or may be liable for assessments. MasterCard recommends that merchants check their checkout process and speak to their service providers on this point.**

---

### Pop-Up Authentication Windows

MasterCard **prohibits** this type of implementation.

### Inline Windows

Inline window implementations, which have proven to virtually eliminate the issues caused by pop-up authentication windows, are required for all new merchant implementations. Existing pop-up implementations must convert to inline windows. By presenting a full-page view, the MasterCard *SecureCode* authentication process appears to be a seamless part of the merchant checkout process, particularly when the merchant uses the “with frames” approach described in the following paragraphs.

### With Frames

A frame implementation allows the merchant to display a branded header and explanation text that can assist cardholders who are new to the MasterCard *SecureCode* experience. In a frame implementation, only part of the full window is redirected to the issuer's access control server.

MasterCard provides the following guidelines and specifications for merchants that choose to implement the frames approach:

- The use of active HTML links in the branded header frame is not allowed. MasterCard recommends including a link below the header frame that directs the cardholder back to the checkout page in case of technical difficulties.
- The explanation text should be clear and concise. The text should not assume that the cardholder is already enrolled in MasterCard *SecureCode* and should not provide instructions that might conflict with the cardholder's issuer instructions.
- The merchant should ensure that the authentication window frame is fully visible and is not located too low in the page because of long text or large upper frame. A minimum space of 400 x 400 pixels is required for the ACS frame.
- Merchants must ensure that the “back” button functionality works properly and that cardholders will be routed back to the checkout page.

### Without Frames

MasterCard research and feedback suggests that cardholders are uncomfortable with the without frames method, therefore it can cause a higher abandonment rate. The use of frames adds the sense of security that the cardholder is still at the merchant site and is not being “phished.” MasterCard recommends that this approach is not used. Any merchant currently supporting this cardholder experience is encouraged to move to a “frame” experience.

## TERMURL Field

The TERMURL is a field that is provided by the merchant to the issuer during the payer authentication request process. This field provides the issuer with the merchant URL where the payer authentication response message is to be sent. The use of mixed HTTP and HTTPS frames typically results in a security box being presented to the cardholder. Depending on how the cardholder responds to this dialog, the current and all future attempts to transmit the PAREq message may fail.

---

### NOTE

**Therefore, merchants using inline authentication windows with frames must populate the TERMURL field with an HTTPS address.**

---

## Replay Detection

Many issuer access control servers attempt to detect replay attacks by not allowing a transaction with the same account ID and XID to be processed more than once. Merchants must ensure that each Payer Authentication Request (PAREq) contains a unique combination of account ID and XID.

## Merchant Server Plug-In Configuration

Following is server plug-in information for merchants.

### Initialization of MasterCard Directory URL

Each merchant endpoint must configure the MPI software to communicate with the MasterCard *SecureCode* Directory server.

### Initialization of MPI Processing Timers

Following is information about cache expiration timers and transaction time-out timers.

#### Cache Expiration Timers

MasterCard recommends that merchants send a VReq to the directory for each transaction rather than using caching to verify card range participation in the program.

For merchants that still use caching, the cache expiration period determines how often cached directory entries must be updated. MasterCard requires that it be updated no sooner than every eight hours and no later than every 24 hours. The updates must not be performed at a specific time every day in order to allow requests to the MasterCard directory to spread out through the day.

---

#### NOTE

**A full refresh of a cache should only be undertaken when absolutely necessary, for example, in the case of an MPI restart. In all other cases a partial cache request should be used.**

---

#### Transaction Time-out Timers

Transaction time-out periods determine how long to wait for a response to a Verification Request message and a Payer Authentication Request message. In the case of PReq/PRes processing specifically, the wait times may vary because of the requirement for cardholder interaction. In practice, however, many financial institutions are using existing consumer credentials (for example, home banking passwords) for the MasterCard *SecureCode* program. As such, issues related to time consuming functions such as forgotten passwords are minimized.

MasterCard recommends the following best practices regarding time-out values:

Function	Time-out Values	Action if timer expires prior to receipt of response
Verify Enrollment Request	20 Seconds	Continue as if the cardholder is not enrolled in the program (for example VERes transaction status = "N")
Payer Authentication Request	MasterCard requires that the merchant allow a minimum of five minutes for return of the PAREs, and recommends that the merchant allow up to 10 minutes for return of the PAREs.	Continue as if cardholder authentication failed (for example PAREs transaction status = "N")

## Initialization of MPI Processing Parameters

There are a number of MPI configuration parameters which, if not set properly, may cause 3-D Secure protocol violations.

All merchants must ensure that their implementation plans account for the following field restrictions:

- The merchant name within any applicable message must be less than or equal to 25 characters including spaces.
- The merchant URL field in the PAREq message must be fully qualified and, ideally, should be the URL of the merchant home page. Many ACS providers present this URL to cardholders, including an active HTML link that directs cardholders to this address.
- The merchant country code must be a valid, 3 digit, ISO 3166 country code.
- The purchase currency code must be a valid, 3 digit, ISO 4217 currency code.

## TERMURL

Merchants must ensure that the TERMURL used for testing is modified to properly reflect the production environment. In addition, the TERMURL field must be fully-qualified.

## Zero or Empty Parameters

Merchants **must** make sure that all parameters sent to the ACS are valid and, unless otherwise indicated by the 3-D Secure protocol, do not contain zero or empty data elements.

For example:

1. The transaction amount should contain a non-zero amount. While technically allowed, sending zeros may cause mishandling of the transaction by the ACS.

2. As defined by the protocol, the MD field must **always** be provided, even if it is not used.
3. If optional fields are not used, MasterCard recommends they be excluded from the message instead of using empty data elements.

## Operational

Following are MasterCard *SecureCode* operational guidelines for merchants.

### Loading of MasterCard Root Certificates

Merchant endpoints are required to load all active and pending MasterCard Root hierarchy certificates. This root will be required by the merchant plug-in to perform digital signature validation. It may also be required in order to establish SSL sessions using certificates based on the MasterCard private hierarchy.

#### NOTE

---

**Currently, MasterCard has two active root certificates that must be loaded.**

---

### Loading of MasterCard SSL Client Certificate

Merchant endpoints are responsible for obtaining all necessary SSL client and server certificates for use by the MPI platform. Individual merchants will be required to use a single MasterCard hierarchy SSL client certificate for their acquirer. If a processor is using the merchant plug-in, MasterCard does not require an individual certificate for each merchant. However, the processor will be required to use a separate and distinct client certificate for each applicable acquirer.

For more information about certificate requirements and procedures, see [Chapter 3, Component Certificate Requirements and Authentication Options](#).

### MPI Log Monitoring

Merchant endpoints should establish a policy of monitoring MPI logs for various authentication failure messages, including signature validation failures. Repeated failures should be reported to the merchant's acquirer. Merchants should note that this could be an indication of issues surrounding the MasterCard *SecureCode* implementation with possible loss of Liability Shift or cost benefits on these transactions.

### MPI Authentication Request/Response Archival

Merchants, or merchant endpoints, should establish a policy for archival of authentication request and response messages. MasterCard recommends that the archival period for this data be the same as the associated authorization transaction data, and should be a minimum of 180 days.

## Accountholder Authentication Value (AAV) Processing

The following processing steps are required by the 3-D Secure protocol and typically handled by the MPI. Any subsequent processing is the responsibility of the merchant.

### Identification of SPA AAV Format in PAREs

The CAVV algorithm field in the PAREs message indicates the algorithm used to create the cryptogram contained in the CAVV field. All MasterCard AAV values will be identified with a value of 3 (MasterCard SPA Algorithm). This is the only value that is permitted for MasterCard and Maestro card transactions.

### Validation of Payer Authentication Response (PAREs) Signature

All PAREs messages returned to the merchant are digitally signed by the associated cardholder's issuer ACS using certificates provided by MasterCard. The merchant is required to validate the signature prior to extracting the SPA AAV from the PAREs message for inclusion in the authorization request sent to the acquirer.

The AAV value in the PAREs must be considered unusable if the signature validation process fails.

## Global Infrastructure Testing Requirements

**All merchant endpoints are required to complete MasterCard *SecureCode* functional testing. This includes execution of the MasterCard *SecureCode* System Test Agreement, when applicable, as well as remittance of applicable fees.**

The purpose for this testing, which only encompasses cardholder authentication testing, is to ensure that merchant implementations meet minimum functional and brand requirements for participating in the MasterCard *SecureCode* program. Any additional authorization testing should be coordinated through the appropriate merchant acquirer or processor.

For additional information on the MasterCard *SecureCode* testing process, send a request via e-mail to [securecode@mastercard.com](mailto:securecode@mastercard.com).

## MasterCard Site Data Protection Program

The MasterCard Site Data Protection Program (SDP) represents a critical piece in the MasterCard comprehensive approach to payment card security. All merchants impacted by the SDP mandate must demonstrate compliance with the Payment Card Industry Data Security Standard (PCI-DSS) security requirements to their acquirer. For additional information about SDP, contact your acquirer or visit [www.mastercard.com/sdp](http://www.mastercard.com/sdp).

## Merchant Processing Matrix

The table below illustrates merchant behavior during various potential scenarios associated with MasterCard *SecureCode* authentication request processing. All information in this table is current.

### Formatted File Type

To access the Merchant Processing Matrix in an Excel® format that can be copied and used as needed, [click here](#). This file can be saved to a local drive for later use.

### MasterCard SecureCode Merchant Process and Liability Shift Matrix

Authentication Scenario	Authentication Process							Notes	Authorization Process			
	VEReq Sent?	VERes Status	PAReq Sent?	PARes			Authorization Processing		Banknet DE48		Liability Shift (See Note)	
				Status	ECI	AAV			SE42	SE43(UCAF)	Merchant-Only	Fully Authenticated
Auth Success	Yes	Y	Yes	Y	02	Yes	Yes		2-1-2	Yes	Yes	Yes
Auth Success (without AAV)	Yes	Y	Yes	Y	02	No	Yes		2-1-1	No	Yes	No
Auth Failure (SecureCode failure)	Yes	Y	Yes	N	-	No	No	1	2-1-0*	No	No	No
Auth Failure (Signature verification incorrect)	Yes	Y	Yes	All	All	All	No	1	2-1-0*	No	No	No
Unable to Authenticate	Yes	Y	Yes	U	-	No	Merchant Optional	3	2-1-1	No	Yes	No
Attempt	Yes	Y	Yes	A	01	Yes	Yes	2	2-1-1	No	Yes	No
Attempt (without AAV)	Yes	Y	Yes	A	01	No	Yes		2-1-1	No	Yes	No
Cardholder Not Participating	Yes	N	No	-	-	-	Yes		2-1-1	No	Yes	No
Unable to Authenticate	Yes	U	No	-	-	-	Yes		2-1-1	No	Yes	No
Cardholder Not Participating (via directory cache)	No	-	-	-	-	-	Yes		2-1-1	No	Yes	No
DS does not respond to MPI	No	-	-	-	-	-	Yes		2-1-1	No	Yes	No
Error on VEReq	Error	-	No	-	-	-	Merchant Optional	3	2-1-1	No	Yes	No
Error on VERes	Yes	Error	No	-	-	-	Merchant Optional	3	2-1-1	No	Yes	No
Error on PARes	Yes	Y	Yes	-	Error	-	Merchant Optional	3	2-1-1	No	Yes	No
Merchant Not SecureCode-enabled	-	-	-	-	-	-	Yes		2-1-0	No	No	No

**Banknet DE 48:**

These indicators map to MasterCard authorization specification requirements for acquirers and issuers. SE42 is the Security Level Indicator and SE43 is the UCAF Data, which contains the AAV. Merchants must refer to the appropriate acquirer or payment processor message specifications for specific formatting requirements.

**Liability Shift**

With effect from October 2011 MasterCard has a global Merchant Only Liability shift in place. For up to date information on chargebacks and liability for personal and commercial cards always refer to the current chargeback guide.

**Notes:**

(1) Best practice would suggest that fraud may be involved and the merchant should prompt the consumer to try again or to use a different form of payment. If merchant decides to send for authorization, the transaction is not eligible for the liability shift and must therefore be coded as a non SecureCode transaction.

(2) The AAV associated with an attempt must not be included in any subsequent authorization message.

(3) The merchant should check the reason for the error message before deciding whether to proceed with the authorization. Not all reason codes may indicate a failure.

---

## Appendix A Merchant Customer Service Guide

*This appendix provides customer service staff with a general overview of the MasterCard® SecureCode™ service, along with an understanding of the consumer experience, in order to provide assistance to customers when needed. This publication is designed for customer service staff at e-retailers that support MasterCard SecureCode.*

---

Frequently Asked Questions.....	A-1
MasterCard <i>SecureCode</i> .....	A-1
What is MasterCard <i>SecureCode</i> ? .....	A-1
What is a MasterCard <i>SecureCode</i> ? .....	A-1
What is the Format of a MasterCard <i>SecureCode</i> ? .....	A-1
Why is our Web site Supporting MasterCard <i>SecureCode</i> ? .....	A-2
How does our Web site Support MasterCard <i>SecureCode</i> ? .....	A-2
What is a Personal Greeting? .....	A-2
What is the Difference between Authentication and Authorization?.....	A-2
How does MasterCard <i>SecureCode</i> work?.....	A-2
What is the Difference between a Pop-up and an Inline Authentication Window? .....	A-3
How does our Web site know if a Card is Protected by MasterCard <i>SecureCode</i> ? .....	A-3
Who knows the Consumer’s MasterCard <i>SecureCode</i> ?.....	A-3
What are the Consumer’s System Requirements for MasterCard <i>SecureCode</i> ? .....	A-3
How Does a Consumer Enroll in the MasterCard <i>SecureCode</i> Program? .....	A-4
What Information is contained on the MasterCard <i>SecureCode</i> Authentication Window? .....	A-4
Will the Authentication Window Appear if the Consumer Never Enrolled in the MasterCard <i>SecureCode</i> Program? .....	A-4
What happens if the Consumer does not know their MasterCard <i>SecureCode</i> ?.....	A-4
What Happens if Authentication Fails? .....	A-5
What Happens if the Consumer Does not Choose to Enter his MasterCard <i>SecureCode</i> ? .....	A-5
Cardholder Enrollment.....	A-5
Traditional Cardholder Enrollment .....	A-5
Activation During Shopping .....	A-6
Consumer Buying Scenarios .....	A-6
Authentication—Successful.....	A-7
Authentication—Forgotten MasterCard <i>SecureCode</i> .....	A-8
Authentication—Failed .....	A-9
Authentication—Account Locked .....	A-10
Activation During Shopping (ADS).....	A-11

Activation During Shopping—Opt Out of Enrollment ..... A-12

## Frequently Asked Questions

Merchants should provide these questions and answers in electronic format on their Web site in addition to making them available to call center staff.

### NOTE

---

**All graphics in this document are samples. Actual consumer experiences may vary based on the specific implementation by the e-retailer and the card-issuing bank.**

---

### DEFINITION

---

**Throughout this section, the term “card issuer” refers to the bank or financial institution that issued the MasterCard® card used by the consumer in the transaction.**

---

## MasterCard *SecureCode*

Following are answers to frequently asked *SecureCode* questions.

### What is MasterCard *SecureCode*?

Today, when a consumer makes a purchase from your Web site, there is no way to confirm the consumer’s identity. MasterCard *SecureCode* is a service from MasterCard that provides a mechanism for the consumer’s identity to be validated by the bank that issued the consumer’s card. By doing so, it provides your business with the ability to obtain a payment guarantee similar to what is available in the physical point-of-sale world.

### What is a MasterCard *SecureCode*?

A MasterCard *SecureCode* is a secret password, known only to the consumer, which is used to validate the consumer’s identity. Depending upon the consumer’s bank, the consumer may be asked to enter their “*SecureCode*,” “*SecureCode* Password” or simply “Password.” Regardless, all of these terms refer to the same thing.

### What is the Format of a MasterCard *SecureCode*?

The format of a consumer’s MasterCard *SecureCode* will vary based on the security policy of the consumer’s card-issuing bank. Typically, it will be a combination of between 4 and 10 letters and numbers.

## Why is our Web site Supporting MasterCard *SecureCode*?

MasterCard *SecureCode* gives your Web site a method to securely authenticate the identity of the consumer. In the online world, there is no signed sales receipt and, in the case of a disputed purchase, it is difficult for you to prove that a consumer made a particular purchase. In those instances, your business is liable for 'unauthorized purchase' fraud. By asking a consumer for a *SecureCode*, and obtaining confirmation from the consumer's card issuer, your business can obtain a guarantee against certain types of fraud. In addition, MasterCard consumer research has shown that consumers are more confident shopping at Web sites that support MasterCard *SecureCode*.

## How does our Web site Support MasterCard *SecureCode*?

To participate in MasterCard *SecureCode*, your Web site has new functionality that works to connect consumers with the card issuer so that the consumer's identity can be validated each time a purchase is made. Your Web site group may have decided to purchase and operate Merchant Plug-in software from an outside vendor. Alternatively, your Web site may be communicating with a server that runs the software program. Depending on the implementation, there are times when consumers may be presented with vendor-specific error codes. Your technical support staff should consult with your vendor or service provider for a list of these codes.

## What is a Personal Greeting?

The Personal Greeting is a message that the consumer creates when registering for the card issuer's MasterCard *SecureCode* program. During an online purchase, the Personal Greeting will appear in the pop-up box from the card issuer. For the consumer's assurance, the Personal Greeting verifies that the consumer is communicating with, and submitting the MasterCard *SecureCode* to, the card issuer.

## What is the Difference between Authentication and Authorization?

Authentication is the process of validating a consumer's identity prior to completing the purchase. MasterCard *SecureCode* is a cardholder authentication program.

Authorization is the process of obtaining approval from the credit card issuing bank for a specific purchase.

## How does MasterCard *SecureCode* work?

First, a consumer must register and create a MasterCard *SecureCode*. Each time an online purchase is made at a participating e-retailer, a window will automatically appear asking for the MasterCard *SecureCode*. MasterCard requires this window to be part of the existing browser display and does not permit the use of pop-up windows for cardholder authentication purposes. The exact implementation is controlled by your Web site.

After reviewing the details of the purchase and confirming that the Personal Greeting is correct, the consumer simply enters the appropriate MasterCard *SecureCode* to complete the purchase. When the consumer correctly enters the MasterCard *SecureCode*, the card issuer confirms the authorized user of that card and provides your Web site with a piece of data, called the accountholder authentication value (AAV), which proves that the authentication was successful. This value must be added to the credit card authorization request to prove that authentication was performed. If a consumer does not enter the correct MasterCard *SecureCode*, the card issuer cannot confirm the identity, and no authentication token is provided. In this particular instance, the online merchant should ask the consumer for an alternative form of payment.

### **What is the Difference between a Pop-up and an Inline Authentication Window?**

The MasterCard *SecureCode* program is designed so that the merchant is responsible for creating the authentication window and the card issuer is responsible for the content of this window. Merchants create an inline window, which will appear as part of the current browser session. MasterCard no longer permits the use of a pop-up window for cardholder authentication because of the prevalence of pop-up blocking software.

### **How does our Web site know if a Card is Protected by MasterCard *SecureCode*?**

When a consumer uses a card that is enrolled in MasterCard *SecureCode* at your Web site, the MasterCard *SecureCode* software (the merchant plug-in, or MPI) automatically makes an inquiry to MasterCard, which will check with the consumer's card-issuing bank. If the consumer is participating, the card issuer will open up a secure dialog with the consumer. This dialog will enable confirmation of the identity of the consumer and, assuming the correct MasterCard *SecureCode* is entered, guarantee the purchase to the merchant.

### **Who knows the Consumer's MasterCard *SecureCode*?**

The MasterCard *SecureCode* value is known only by the consumer and the consumer's card-issuing bank. The dialog during which the consumer enters the MasterCard *SecureCode* value takes place with the issuing bank only. No other parties, including your Web site or MasterCard, are involved in this process. Your Web site is simply notified of the result of this process via the MasterCard *SecureCode* software.

### **What are the Consumer's System Requirements for MasterCard *SecureCode*?**

MasterCard *SecureCode* works with most browsers. If the consumer has any difficulty performing authentication, he should contact his card issuer's customer service by calling the phone number on the back of his card.

## How Does a Consumer Enroll in the MasterCard *SecureCode* Program?

Refer to [Cardholder Enrollment](#) in this chapter for information.

## What Information is contained on the MasterCard *SecureCode* Authentication Window?

The authentication window is similar to the receipt that consumers sign in a store. It includes details such as where the purchase is being made and how much money is being spent. The actual content of this window is provided by the consumer's card issuing bank based on information provided by your Web site.

## Will the Authentication Window Appear if the Consumer Never Enrolled in the MasterCard *SecureCode* Program?

There are two situations where the authentication window may appear—both of which are related to the enrollment process.

- A MasterCard *SecureCode* has been selected by one authorized user and not communicated to the other authorized users on the account. For example, husband and wife. Most card issuers do provide the ability for each authorized user of the card to individually enroll and establish his/her own MasterCard *SecureCode*. In that case, the *SecureCode* value for either user may complete the authentication process.
- The card issuer tries to enroll the consumer using Activation During Shopping. Refer to [Activation During Shopping](#) in this chapter for more information.

## What happens if the Consumer does not know their MasterCard *SecureCode*?

It varies by card-issuing bank but consumers are usually given three chances to successfully enter the MasterCard *SecureCode*. An invalid attempt will result in a prompt to the consumer to try again. In the event that a consumer forgets the MasterCard *SecureCode*, most card issuers provide an alternative mechanism to complete the authentication process. Typically, there is a “Forgot my *SecureCode*” link that the consumer can click to obtain assistance.

After the allowable number of tries has been exceeded, the card-issuing bank may prompt the consumer with a series of questions to authenticate his identity—for example, last four digits of social security number, birth date, signature panel code on card, and more. If this information is successfully validated, a successful authentication response will be returned to your Web site. If not, the account will most likely be locked to prevent any further authentication attempts at your Web site and also at other participating Web sites.

Refer to [Authentication—Forgotten MasterCard \*SecureCode\*](#) in this chapter for additional information.

## What Happens if Authentication Fails?

The result of a failed authentication depends on how your particular Web site has been set up. At some Web sites, a failed authentication will cause the e-retailer to request a different payment method before allowing the purchase to proceed. In other cases, the transaction may be submitted for authorization as a non-MasterCard *SecureCode* transaction.

Refer to [Authentication—Failed](#) in this chapter for additional information.

## What Happens if the Consumer Does not Choose to Enter his MasterCard *SecureCode*?

Depending upon the particular card issuer's MasterCard *SecureCode* program implementation, consumers may either be required to authenticate themselves or they will be given the option of canceling the process. When a consumer chooses to cancel from the process, an alert is displayed providing the option to return to the authentication window to continue the authentication process.

Selecting **OK** will return the consumer back to the previous authentication window. Selecting **Cancel** will terminate the authentication window and return an authentication failed status indicator back to your Web site. Your Web site implementation will determine what next is presented to the consumer. Some e-retailers will continue with the authorization as a non-SecureCode transaction. Others choose not to accept payment from cards that fail authentication, and instead ask for a different form of payment.

# Cardholder Enrollment

Enrollment is the process whereby eligible MasterCard and Maestro branded cardholders will activate their cards for use in the program.

This process typically occurs in one of two ways:

- **Traditional Cardholder Enrollment**—The cardholder will need to go to his issuing bank's Web site to enroll, prior to going shopping.
- **Activation During Shopping**—The cardholder will activate his account during a purchase.

It is important to remember that all enrollments are between the authorized cardholders and their card-issuing banks. MasterCard is not involved in the enrollment process.

## Traditional Cardholder Enrollment

This type of enrollment typically takes place at a Web site designated by the bank that issued the card. For example, it may be the bank's home page or home banking system.

In a typical example:

1. The consumer will be asked to provide enrollment data. During this phase of the process, the consumer will be asked a series of questions to prove identity to their bank. This may include asking for information such as the last four digits of the consumer's social security number, birth date, or the signature panel code from the back of the credit card.
2. The answers to the questions will be validated either in-house at the bank or through a third party processor such as a credit bureau.
3. If the consumer answers the questions correctly, the consumer is considered authenticated and will be allowed to establish the MasterCard *SecureCode* for that particular MasterCard account number. The MasterCard *SecureCode* will be stored by the card issuer for use later on during online purchases at participating e-retailers.

## **Activation During Shopping**

Unlike the traditional enrollment process, Activation During Shopping (ADS) does not require the consumer to visit an enrollment Web site before shopping. This type of enrollment, which has proven to be very successful, takes place during the shopping process. When an eligible consumer goes to checkout, the card-issuing bank will ask a series of questions—similar to the traditional enrollment process. Providing the correct answers will result in both a successful enrollment and a successful authentication response returned to your Web site. Refer to [Consumer Buying Scenarios](#) in this chapter to for a sample shopping scenario.

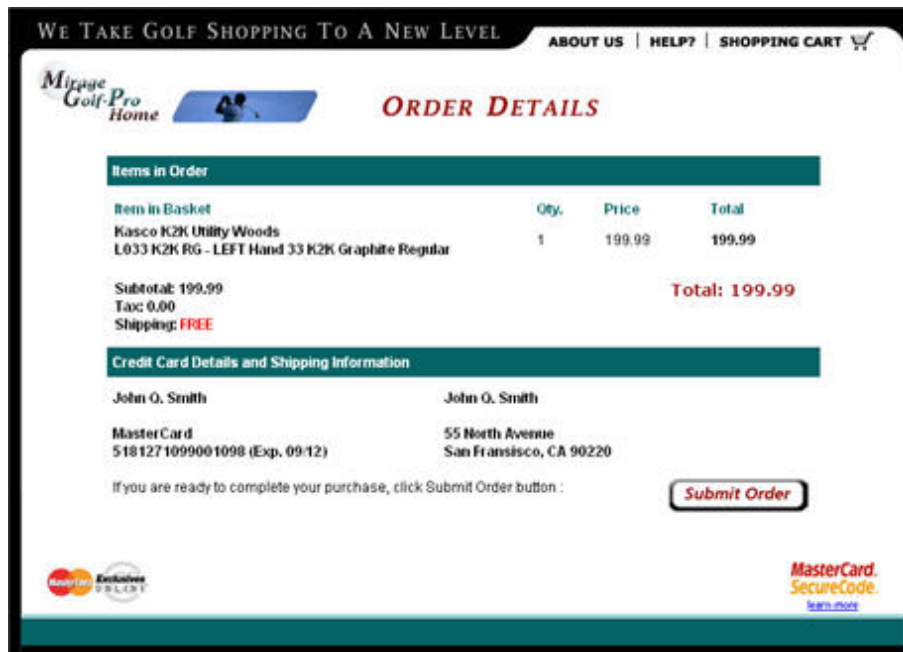
## **Consumer Buying Scenarios**

The following section provides sample screen shots of several consumer scenarios that may be encountered while shopping at your Web site. Each of these scenarios occurs after the consumer elects to submit the order but prior your site actually initiating a request to authorize the transaction.

Each of the scenarios begins at the point where this particular e-retailer is asking for final confirmation of the purchase.

Actual screen content will most likely vary from the samples depicted.

Figure A.1—Final Purchase Confirmation



## Authentication—Successful

In this scenario, the consumer is presented with the authentication window as seen below. After entering the proper MasterCard *SecureCode*, a message will be returned to your Web site indicating the authentication was performed successfully. At this point, your Web site will send the fully authenticated authorization request to MasterCard for approval. An approved response for qualified requests will result in a payment guarantee to your company.

Figure A.2—Enter Your MasterCard *SecureCode* Window

**MEMBER BANK** **MasterCard SecureCode.**

**Enter Your SecureCode™**

Please enter your MasterCard® SecureCode™ in the field below to confirm your identity for this purchase. This information is not shared with the merchant.

Merchant: Sample SDK Implementation

Amount: **14,748.00 USD**

Date: 09:05:07

Card number: XXXX XXXX XXXX 0035

Personal Greeting: MC Staging

SecureCode:

[Forgot your SecureCode?](#)

**Submit** ▶

[Help](#) [Cancel](#)

## Authentication—Forgotten MasterCard *SecureCode*

In this scenario, the consumer is presented with the authentication window to begin the process. However, in this case, the consumer does not know their MasterCard *SecureCode*.

In response to not knowing his MasterCard *SecureCode*, the consumer clicks the “Forgot Your SecureCode” link. See [Figure A.2](#) for an example.

The following screen appears after the consumer clicks the **Forgot Your SecureCode** link:

Figure A.3—Forgot Your SecureCode? Window

**MEMBER BANK** **MasterCard SecureCode.**

**Forgot Your SecureCode™?**  
If you have forgotten your SecureCode, you can reset it once you have verified your identity.

Complete the following:

**Signature Panel Code\***  [What is this?](#)

**Expiration date\***

**5-Digit Billing Zip Code\***

To complete this transaction enter your information and click "Continue".

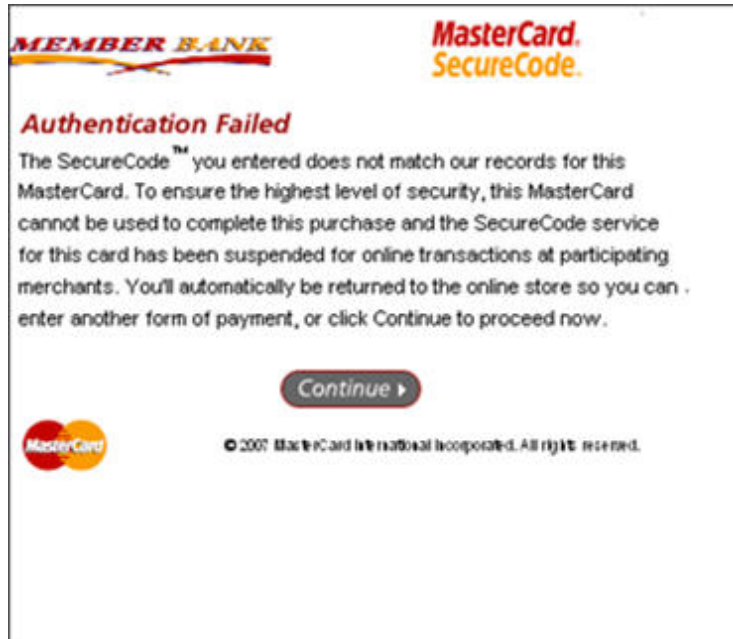
[Continue >](#) [Help](#)

This particular financial institution has decided to tell the consumer that they must call the bank's customer service department for additional help and will return a failed authentication response to the merchant. In other cases, financial institutions will prompt the consumer to answer a series of secret questions. Providing the proper answer to these questions will permit the consumer authentication process to complete successfully.

## Authentication—Failed

In this scenario, the consumer is presented with the authentication window to begin the process (See [Figure A.3](#)). Unlike the previous example, the consumer thinks that they know the MasterCard *SecureCode*. Each subsequent attempt to enter an invalid value will result in an error message on the authentication window.

Figure A.4—Authentication Failed



After a predetermined number of attempts, the card-issuing bank may optionally lock the account and present the consumer with a display indicating that authentication has failed. In addition, the display may give information on how to obtain help in order to reset the MasterCard *SecureCode* value for next time.

Once the account has been locked, it may not be used for shopping at any participating e-retailer. The consumer must use the facilities provided by their card-issuing financial institution to reset the MasterCard *SecureCode*. These may include the bank's customer service and/or MasterCard *SecureCode* enrollment site.

## Authentication—Account Locked

When card-issuing banks detect that potential fraud may be occurring, they will often lock the account to prevent authentication. One example of this is when the consumer unsuccessfully attempts to enter the MasterCard *SecureCode* too many times. When the e-retailer attempts to perform authentication on these accounts, the response back from the card issuer will be that authentication has failed. See [Figure A.4](#) for an example.

## Activation During Shopping (ADS)

Unlike the previous scenarios, this example shows what may happen to a consumer that is not currently enrolled in a card issuer's MasterCard *SecureCode* program. Instead of being provided with a window to enter the MasterCard *SecureCode*, the consumer is provided with a window to enroll in the program and authenticate their identity for the current transaction. This window will typically ask a series of secret questions.

If correct answers are provided to the questions, the merchant will be returned a status indicating that the consumer was successfully authenticated just as if a valid MasterCard *SecureCode* had been entered.

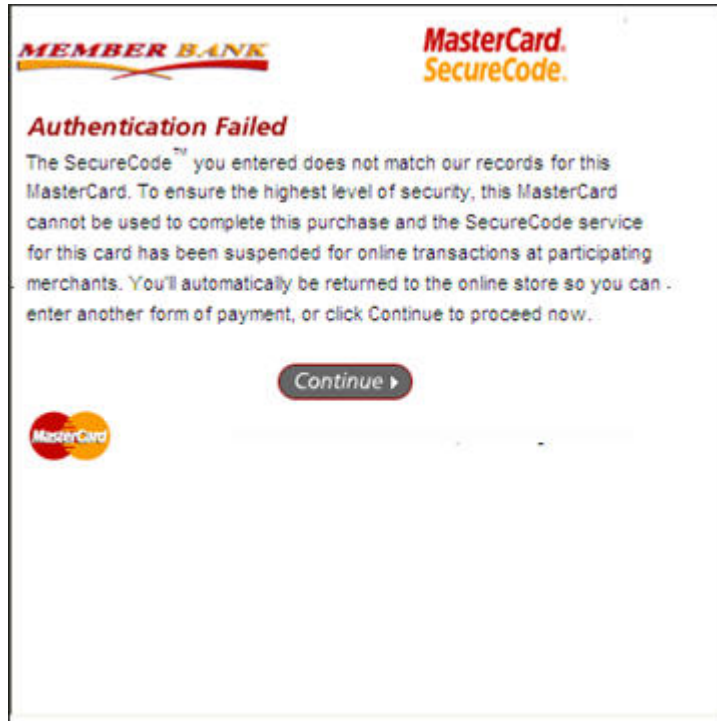
If the incorrect responses are provided to the questions, the consumer will be given at least one more opportunity to provide the appropriate answers.

Figure A.5—Incorrect Answers Message During ADS

The screenshot displays a web interface for MasterCard SecureCode enrollment. At the top left is the 'MEMBER BANK' logo, and at the top right is the 'MasterCard SecureCode' logo. A red error message reads: 'We're sorry, the information you submitted does not match our records. Please submit your information again. If you continue to experience difficulty, please call the number on the back of your MasterCard® card.' Below the message are three input fields: 'Signature Panel Code\*' (a text box with a 'What is this?' link), 'Expiration date\*' (two dropdown menus for 'Month' and 'Year'), and '5-Digit Billing Zip Code\*' (a text box). At the bottom left is a link 'Do not continue', and at the bottom center is a button labeled 'Continue to Step 2' with a right-pointing arrow.

If the consumer chooses not to enroll in the program at the current time, a message will be displayed indicating that the purchase will continue without a MasterCard *SecureCode* value. To your Web site, this means the credit card authorization will be unauthenticated.

Figure A.6—Processing without MasterCard SecureCode Message



If the incorrect responses are provided too many times, or if the issuer requires enrollment and the cardholder declines to enroll, the merchant will be notified that consumer authentication has failed. In this particular case, merchants may either request an alternative form of payment or proceed with a non-MasterCard *SecureCode* authorization request.

## Activation During Shopping—Opt Out of Enrollment

In this scenario, the consumer opts not to enroll in the program at the current time. Instead of providing answers to the questions on the window, the consumer clicks the **Do Not Continue** link.

Figure A.7—Do Not Continue Link

The screenshot shows a web page with the Member Bank logo on the left and the MasterCard SecureCode logo on the right. A red error message reads: "We're sorry, the information you submitted does not match our records. Please submit your information again. If you continue to experience difficulty, please call the number on the back of your MasterCard® card." Below the message are three input fields: "Signature Panel Code\*" with a text box and a "What is this?" link; "Expiration date\*" with "Month" and "Year" dropdown menus; and "5-Digit Billing Zip Code\*" with a text box. At the bottom, there is a link "Do not continue" and a prominent button labeled "Continue to Step 2 ▶".

At this point in time, the e-retailer will be notified that the consumer declined to enroll in the program. In this particular case, the e-retailer should proceed with an unauthenticated authorization using the current card number.

MasterCard recommends that card issuers give cardholders at least three chances to enroll in the MasterCard *SecureCode* program. If the cardholder does not enroll after three chances, some card issuers will not give the cardholder the ability to opt-out of their MasterCard *SecureCode* program, and will, in fact, lock the account and present the consumer with a display indicating that authentication has failed. Once the account has been locked, it may not be used for shopping at any participating e-retailer. The consumer must use the facilities provided by his card issuer financial institution to enroll in *SecureCode*. These may include the bank's customer service center, its MasterCard *SecureCode* enrollment site, or both.

---

## Appendix B MasterCard SecureCode SPA Algorithm Specifications

*This chapter contains the layout of the Accountholder Authentication Value (AAV) to be used by issuers participating in MasterCard® SecureCode™, as well as an overview of Base64 encoding.*

---

Overview .....	B-1
Accountholder Authentication Value Layout .....	B-1
Base64 Encoding .....	B-1
Introduction .....	B-1
Examples .....	B-2
AAV Control Byte hexadecimal “8C” (Successful cardholder authentication) .....	B-2
AAV Control Byte hexadecimal “86” (Attempted cardholder authentication).....	B-2
Base64 Alphabet .....	B-3

---

## Overview

This chapter includes the layout of the Accountholder Authentication Value (AAV) defined for use with MasterCard® *SecureCode*™. It also contains a brief overview of Base64 encoding.

## Accountholder Authentication Value Layout

The format of the AAV is defined and described in the SPA Algorithm for the MasterCard Implementation of 3-D Secure publication. This is a licensed publication available only to MasterCard members or any non-member that has successfully executed the MasterCard *SecureCode* license agreement.

## Base64 Encoding

The following overview of Base64 encoding is taken from RFC1521 “*Mime (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies*”. For more detailed information, please refer to [www.ietf.org/rfc/rfc1521.txt?number=1521](http://www.ietf.org/rfc/rfc1521.txt?number=1521).

### Introduction

Base64 encoding is designed to represent arbitrary sequences of octets in a form that need not be humanly readable. The encoding and decoding algorithms are simple, but the encoded data are consistently about 33 percent larger than the unencoded data.

A 65-character subset of US-ASCII is used, enabling 6 bits to be represented per printable character. The extra 65<sup>th</sup> character, “=”, is used to signify a special processing function.

The encoding process represents 24-bit groups of input bits as output strings of four encoded characters. Proceeding from left to right, a 24-bit input group is formed by concatenating three 8-bit input groups. These 24 bits are then treated as four concatenated 6-bit groups, each of which is then translated into a single digit in the Base64 alphabet. When encoding a bit stream via the Base64 encoding, the bit stream must be presumed to be ordered with the most-significant-bit first. That is, the first bit in the stream will be the high-order bit in the first byte and the eighth bit will be the low-order in the first byte, and so on.

Each 6-bit group is then used as an index into an array of 64 printable characters. The character referenced by the index is placed in the output string. These characters, identified by Base64 Alphabet, are selected so that they are universally representable. The set excludes characters with particular significance to SMTP (for example: “.”, CR, LF).

## Examples

The following examples will perform the beginning steps of Base64 encoding of an AAV control byte field. The encoding process for the remainder of the AAV will follow the same process.

The decoding process will simply work in reverse.

### AAV Control Byte hexadecimal "8C" (Successful cardholder authentication)

Displaying hexadecimal 8C in its binary equivalent gives the following:

1 0 0 0 1 1 0 0

The data is then broken down into three 24-bit segments, which are interpreted as four 6-bit segments for encoding. In this case, the first 6 bits equal:

1 0 0 0 1 1

Converting this to its decimal equivalent yields the following:

$$(1*2^5) + (0*2^4) + (0*2^3) + (0*2^2) + (1*2^1) + (1*2^0)$$

$$32 + 0 + 0 + 0 + 2 + 1$$

Decimal 35 = Base64 j

### AAV Control Byte hexadecimal "86" (Attempted cardholder authentication)

Displaying hexadecimal 86 in its binary equivalent gives the following:

1 0 0 0 0 1 1 0

The data is then broken down into three 24-bit segments, which are interpreted as four 6-bit segments for encoding. In this case, the first 6 bits equal:

1 0 0 0 0 1

Converting this to its decimal equivalent yields the following:

$$(1*2^5) + (0*2^4) + (0*2^3) + (0*2^2) + (0*2^1) + (1*2^0)$$

$$32 + 0 + 0 + 0 + 0 + 1$$

Decimal 33 = Base64 h

---

## Base64 Alphabet

Decimal Value	Encoding	Decimal Value	Encoding	Decimal Value	Encoding	Decimal Value	Encoding
0	A	17	R	34	i	51	z
1	B	18	S	35	j	52	0
2	C	19	T	36	k	53	1
3	D	20	U	37	l	54	2
4	E	21	V	38	m	55	3
5	F	22	W	39	n	56	4
6	G	23	X	40	o	57	5
7	H	24	Y	41	p	58	6
8	I	25	Z	42	q	59	7
9	J	26	a	43	r	60	8
10	K	27	b	44	s	61	9
11	L	28	c	45	t	62	+
12	M	29	d	46	u	63	/
13	N	30	e	47	v	(pad)	=
14	O	31	f	48	w		
15	P	32	g	49	x		
16	Q	33	h	50	y		

---

## Appendix C Contact Information

*This section contains a list of MasterCard contact information.*

---

Contact Information .....	C-1
MasterCard <i>SecureCode</i> Online Resources .....	C-1

## Contact Information

This chapter contains names, areas of responsibility, and contact information for MasterCard® personnel who can assist members with e-commerce enrollment, testing, and implementation issues.

Area of Responsibility	Contact Information
Completed and signed enrollment forms	Send all completed and signed enrollment forms to your MasterCard regional representative. The regional representative will forward the forms to the appropriate electronic commerce representative.
Maestro	<p><b>Customer Operations Services</b>  <b>U.S., Canada, Caribbean, Latin America, South Asia, Middle East, and Africa</b>  <b>Phone:</b> 800-999-0363 (Inside U.S.)  636-722-6176 (Outside U.S.)  636-722-6292 (Spanish Language Support)  <b>Fax:</b> 636-722-7192  <b>E-mail:</b>  <a href="mailto:customer_support@mastercard.com">customer_support@mastercard.com</a></p> <p><b>Europe</b>  <b>Phone:</b> +32-2-352-54-03  <b>E-mail:</b> <a href="mailto:css@mastercard.com">css@mastercard.com</a></p>
Program Management Support Pricing/Billing	<a href="mailto:securecode@mastercard.com">securecode@mastercard.com</a>
Support	<a href="mailto:securecode_support@mastercard.com">securecode_support@mastercard.com</a>

## MasterCard *SecureCode* Online Resources

For additional information about MasterCard® *SecureCode*™, please visit one of the following Web sites:

- **Consumer Web site:** [www.mastercard.com/securecode](http://www.mastercard.com/securecode)
- **Certified SecureCode Vendors:**  
[www.mastercard.com/us/merchant/solutions/securecode\\_vendor\\_list.html](http://www.mastercard.com/us/merchant/solutions/securecode_vendor_list.html)
- **SecureCode FAQs:** [www.mastercard.com/securecd/faq.do](http://www.mastercard.com/securecd/faq.do)
- **Merchant Web site:** [www.mastercardmerchant.com/securecode](http://www.mastercardmerchant.com/securecode)
  - **Merchant FAQs:**  
[www.mastercard.com/us/merchant/assistance/faqs.html#securecode](http://www.mastercard.com/us/merchant/assistance/faqs.html#securecode)
  - **Program Identifier Guidelines:**  
[mastercardmerchant.com/securecode/artwork.html](http://mastercardmerchant.com/securecode/artwork.html)

Also, the e-business section of MasterCard OnLine™ contains additional program information.

---

## Appendix D Maestro Considerations

*This chapter contains detailed information about specific processing issues associated with Maestro® and MasterCard® SecureCode™. Merchants should contact their acquirer for specific authorization and clearing requirements.*

---

Account in Good Standing.....	D-1
-------------------------------	-----

## Account in Good Standing

An account in good standing transaction is a request by a merchant to check the authenticity of a Maestro® account number. Unlike other Maestro transactions, Account in Good Standing is not a financial transaction. It does not perform a value check or guarantee that the customer has sufficient funds to cover the purchase. The objective is to satisfy the merchant's primary concern to ensure that the Maestro card number being provided by the customer is not counterfeit.

Merchants must not confuse an Account in Good Standing transaction with a pre-authorization transaction used for self-service pumps at petrol/gas stations. These transactions are used to guarantee a block of funds up to the amount in the transaction, provided it is followed within 20 minutes by a completion transaction.

An account in good standing transaction is a standard authorization message with the following specific data content requirements.

Data Element	Name	Value
4	Transaction Amount	One unit of purchase currency
61, subelement 7	Point-of-Service Data (POS) Transaction Status Indicator	4 = Preauthorized Request

These data elements must be used by the acquirer when placing an account in good standing transactions. Each acquirer is responsible for determining how this transaction is supported in the point of interaction message defined for the merchant to acquirer interface.

---

## Appendix E India IVR Transactions (SecureTelephone)

*This appendix provides a general overview of the MasterCard requirements to support IVR Transactions in India.*

---

Overview .....	E-1
Data Extensions to the existing 3-D Secure Protocol.....	E-1
UCAF Transport in MasterCard Authorization Messages .....	E-1
MasterCard <i>SecureCode</i> —Security Level Indicator (DE 48, subelement 42) .....	E-2
Universal Cardholder Authentication Field (DE 48, subelement 43).....	E-2
What is Accountholder Authentication Value? .....	E-3
Sample IVR transaction flow.....	E-3
MasterCard <i>SecureCode</i> Compliance and Functional Testing .....	E-4

---

## Overview

Following the successful deployment of 3-D Secure (SecureCode) for all domestic electronic commerce transactions, the banking authority of India, Reserve Bank of India (RBI), has defined a mandate that requires a similar 2-factor authentication process to also be rolled out for IVR transactions.

As there was no technology or precedent of authenticating an IVR transaction with 2-factor authentication, MasterCard has worked with IVR vendors to utilize existing investments in technology, process and infrastructure to build a framework and specification using the 3-D Secure protocol. As owner of the 3-D Secure Protocol, Visa has published a country specific (India) specification that defines a number of additional data elements in the existing 3-D Secure messages.

For additional information, see *3-D Secure Functional Requirements—Extensions for Mobile and IVR Transactions in India v1.1*.

## Data Extensions to the existing 3-D Secure Protocol

As detailed in the *3-D Secure Functional Requirements—Extensions for Mobile and IVR Transactions in India v1.1*, the Verify Enrollment Request (VEReq), VERes and PAREq messaging within the 3-D Secure protocol have been extended to allow the Merchant plug-in (MPI) and Issuer Access Control Server (ACS) to convey the additional transaction related elements that identify an IVR transaction, as opposed to an electronic commerce transaction.

## UCAF Transport in MasterCard Authorization Messages

MasterCard has designated specific subelements within DE 61 (Point-of-Service [POS] Data) and DE 48 (Additional Data—Private Use) for the identification of SecureTelephone Order and transport of UCAF related data and associated indicators in authorization messages. These subelements will be used to support and identify IVR transactions within the authorization message. Support for SecureTelephone Order within the authorization message was mandated as part of the 7.2 Banknet release.

The subelements are described in the following sections. Refer to the *Customer Interface Specification manual* for additional information regarding authorization message formatting.

SecureTelephone—DE 61—Point-of-Service (POS) Data, subelements 4, 7, and 10. The following sub-element values are to correctly identify an IVR (SecureTelephone Order) DE 61.

Subelement	Value	Description
4—POS Cardholder Presence	3	Cardholder Not Present, Phone/ARU Order
7—POS Transaction Status	2	SecureCode Phone Order
10—Cardholder-Activated Terminal Level	MUST NOT BE 6	Authorized Level 6 CAT: Electronic commerce

## MasterCard *SecureCode*—Security Level Indicator (DE 48, subelement 42)

The SecureCode Security Level Indicator contains the fields representing the security protocol and cardholder authentication type associated with the transaction. MasterCard requires that subelement 42 be included and properly populated for all electronic commerce and SecureTelephone (IVR) transaction authorizations.

Please note that only Fully authenticated IVR transactions (Security Level Indicator 2- UCAF data collection is supported by the merchant, and UCAF data is present in DE 48, SE 43) are applicable to SecureTelephone order (IVR) transactions.

The required data values for SecureTelephone order (IVR) are provided in the table below.

Position	Value	Description
1—Security Protocol	2	Channel Encryption (for example, SSL)
2—Cardholder Authentication	1	Cardholder Certificate Not Used
3—UCAF Collection Indicator	<ul style="list-style-type: none"> <li>• 0</li> <li>• 2</li> </ul>	<ul style="list-style-type: none"> <li>• UCAF data collection is not supported by the merchant</li> <li>• UCAF data collection is supported by the merchant, and UCAF data is present (DE 48, subelement 43)</li> </ul>

## Universal Cardholder Authentication Field (DE 48, subelement 43)

The Universal Cardholder Authentication Field (UCAF) contains the encoded MasterCard® *SecureCode*™ issuer-generated authentication data (collected by the merchant) resulting from all MasterCard SecureCode fully authenticated transactions.

UCAF is a standard, globally interoperable method of collecting cardholder authentication data at the point of interaction. Within the MasterCard authorization networks, UCAF is a universal, multipurpose data transport infrastructure that is used to communicate authentication information between cardholders, merchants, issuers, and acquirers. It is a variable length (maximum 32 characters) field with a flexible data structure that can be tailored to support the needs of issuer security and authentication approaches.

**NOTE**

---

**All acquirers and issuers must ensure that they can send and/or receive contents in this field up to the maximum length of 32. Note that applications utilizing this field, such as SecureCode, may provide contents that are less than the maximum length. For MasterCard *SecureCode* specifically, this field will be 28 positions. This field should NOT include any padding to meet the maximum length of 32 bytes.**

---

### **What is Accountholder Authentication Value?**

The Accountholder Authentication Value (AAV) is a MasterCard *SecureCode* specific token that uses the UCAF field for transport within MasterCard authorization messages. It is generated by the issuer and presented to the merchant for placement in the authorization request upon successful authentication of the cardholder.

In the case of a chargeback or other potential dispute processing, the AAV will be used to identify the processing parameters associated with the transaction. Among other things, the field values will identify the:

- Issuer ACS that created the AAV.
- Sequence number that can be used to positively identify the transaction within the universe of transactions for that location.
- Secret key used to create the Message Authentication Code (MAC), which is a cryptographic method that not only ensures AAV data integrity but also binds the entire AAV structure to a specific PAN.

### **Sample IVR transaction flow**

1. Cardholder calls the merchant to order items, and finalize purchase.
2. Merchant collects all necessary data, including PAN and cardholders phone information.
3. The merchants modified IVR-MPI creates a Verify Enrollment Request (VEReq) message with the IVR extensions, including the following data:
  - a. Format of Phone number or Device ID
  - b. Cardholder Phone number or Device ID
  - c. PAREq channel—DIRECT
  - d. Shopping Channel—IVR
  - e. Available Authentication Channels
4. The MasterCard Directory Server will forward VEReq to the appropriate Issuer IVR-ACS, to validate that the PAN is enrolled in the service.
5. The issuer IVR-ACS responds to the MasterCard Directory with confirmation of enrollment, and the VERes including the ACS URL is returned to the Merchant IVR-MPI.

6. IVR-MPI generates a PAREq message with the IVR extension, and sends to the appropriate Issuer IVR-ACS.
7. ACS receives and processes the PAREq message—IVR extensions may be used by the Issuer ACS in the authentication process.
8. Upon successful validation of the cardholder (or using data contained in the extended PAREq), the issuer ACS will generate the PAREs message and forward to Merchant IVR-MPI.
9. IVR-MPI receives PAREs and proceeds with authorization request.

### **MasterCard SecureCode Compliance and Functional Testing**

Proof of Visa Certification of IVR-ACS and IVR-MPI development is required before MasterCard compliance testing can commence

MasterCard has developed compliance testing, for issuer and merchant functional testing, to ensure vendor products and member and merchant implementations are compliant and successfully interoperate with all MasterCard SecureCode platforms and infrastructure.

All vendors, merchant-end points, and issuers are required to complete the designated testing process prior to launch.

Request additional information about testing by sending a message to [securecode@mastercard.com](mailto:securecode@mastercard.com).

---

## Appendix F MasterCard Advance Registration Program

*This appendix introduces the MasterCard Advance Registration Program (MARP) and identifies the program requirements.*

---

MasterCard Advance Registration Program .....	F-1
Participation Requirements for Merchants .....	F-1
MARP Merchant Use of MasterCard <i>SecureCode</i> .....	F-2
Acquirer Impact .....	F-3

## MasterCard Advance Registration Program

MasterCard Advance Registration Program (MARP) was introduced for Maestro in 2008, and for MasterCard in 2010. MasterCard has reminded issuers that the support of MARP is mandatory and that issuers cannot selectively accept only the full MasterCard® *SecureCode*™ transactions.

Further, MasterCard is also introducing a simplified structure for Static AAVs used to support the program to minimize the long term impact of the program on issuers.

The program is designed to encourage participating merchants to implement MasterCard *SecureCode* and use it as part of a risk-based authentication strategy for high-risk e-commerce transactions. This provides the merchants with flexibility and control over the check-out experience. Valid e-commerce transactions under MARP can be initiated through a mobile device or a computer.

To participate, a merchant must demonstrate a commitment to ensuring both a positive customer checkout experience and a robust risk management system.

### Participation Requirements for Merchants

MARP is open to e-commerce merchants that accept MasterCard cards, Maestro cards, or both, and that provide customers with a positive, secure e-commerce shopping experience. For each merchant, the acquirer will complete a participation request form designed to help MasterCard understand the merchant's e-commerce acceptance environment. MasterCard staff will review the participation request form, and notify the acquirer if the merchant has been enrolled in the program.

To be eligible for this program the merchant must **enable its customers to register on the merchant's Web site** by selecting a username and password or similar credentials, and provide cardholders with the option to register a MasterCard or Maestro card number for use in future e-commerce transactions. The merchant will also be expected to satisfy minimum **security requirements** intended to help ensure the protection of all participants: the merchant, its acquirer, the issuer, and the cardholder. The merchant must offer customers a safe, secure shopping experience by using best practice risk management tools. In addition, the merchant must demonstrate a commitment to conducting business in a manner that does not result in excessive chargebacks. More information about the program, including the program terms and the merchant enrollment process, are available on MasterCard OnLine®. From the **Main Menu**, select **e-Business**, then **e-Commerce**, and then click **MasterCard and Maestro Advance Registration Program**.

## MARP Merchant Use of MasterCard SecureCode

MARP enables enrolled merchants to authenticate e-commerce transactions as follows:

- The merchant invites the customer to register on its Web site by choosing a username and password, or similar credentials acceptable to MasterCard, and must provide the customer with the option to register a MasterCard or Maestro card account number for use in future e-commerce transactions.
- For the first MasterCard or Maestro e-commerce transaction, the merchant must request MasterCard *SecureCode* authentication before submitting the transaction for authorization. If that transaction is subsequently authorized by the issuer, it is guaranteed to the acquirer or its merchant, regardless of whether the issuer or cardholder participates in MasterCard *SecureCode* as determined by the merchant request.
- If the first MasterCard or Maestro e-commerce transaction for the cardholder registered with the merchant is authorized by the issuer, the merchant can skip the MasterCard *SecureCode* authentication on subsequent transactions by the same customer using the same MasterCard or Maestro card account.

In that case, the merchant will populate:

- The MasterCard Assigned ID (DE 48, subelement 32) in the Authorization Request/0100 message with a MasterCard-assigned ID.
- The UCAF (DE 48, subelement 43) in the Authorization Request/0100 message with a MasterCard-assigned static Account Authentication Value (AAV).
- The UCAF Collection Indicator (DE 48, subelement 42, position 3) in the Authorization Request/0100 message with a value of 3.
- The UCAF Collection Indicator (PDS 0052, subfield 3 ) in the clearing record submitted to GCMS for processing (where applicable) with a value of 3.
- The MasterCard Assigned ID (PDS 176) in the clearing record submitted to GCMS for processing with a MasterCard-assigned ID.
- If the merchant populates the UCAF with the static AAV assigned by MasterCard, and populates the UCAF Collection Indicator with the value of 3, and the issuer authorizes the transaction, the issuer will have a right to charge back the transaction for reason of fraud.
- If a registered cardholder uses a different MasterCard or Maestro card account number for a transaction, the merchant must request MasterCard *SecureCode* authentication before submitting the transaction for authorization.
- Based on a risk assessment the merchant always has the option of requesting MasterCard *SecureCode* authentication for any MasterCard or Maestro transaction, in which case the transaction will be governed by existing MasterCard *SecureCode* and Chargeback rules. For instance, for consumer cards acquired in the Europe region, if the transaction is subsequently authorized by the issuer, it is guaranteed to the acquirer or its merchant, regardless of whether the issuer or cardholder participates in MasterCard *SecureCode* as determined by the merchant request.

## Acquirer Impact

Participation in MARP is optional for Europe region acquirers. Acquirers outside the Europe region are not eligible to participate in the program.

Effective 9 November 2010:

- Acquirers authorization systems must support a value of 3 in the UCAF Collection Indicator (DE 48, sub element 42, position 3) in the Authorization Request/0100 message.
- Acquirers may submit qualifying transactions with the UCAF Collection Indicator (PDS 0052, subfield 3) in the First Presentment/1240 message containing a value of 3 and with an Interchange Rate Designator (IRD) applicable for the Full-UCAF Interchange Tier, as defined in the *Interchange and Service Fees—Europe Region* manual.

Acquirers that would like to enroll a merchant for the program may do so by following the enrollment process that is available on MasterCard OnLine®. From the **Main Menu**, select, **e-Business**, then **e-Commerce**, and then click **MasterCard and Maestro Advance Registration Program**.