Information about this Replacement

Replacement	The November 2007 *POS Terminal Security Program – Program Manual* replaces your existing manual dated July 2006.
What is in the new version?	This new version reflects the experienced gained in operating the POS Terminal Security Program to date, and the comments received from both vendors and evaluation laboratories. Please refer to: • "Summary of Changes" for a comprehensive list of changes reflected in this update. • "Using this Manual" for a complete list of the contents of this manual.
Questions?	If you have questions about this manual, please contact the Customer Operations Services team or your regional help desk. Please refer to "Using this Manual" for more contact information.
MasterCard is Listening…	Please take a moment to provide us with your feedback about the material and usefulness of the *POS Terminal Security Program – Program Manual* using the following e-mail address: publications@mastercard.com We continually strive to improve our publications. Your input will help us accomplish our goal of providing you with the information you need.

Summary of Changes

POS Terminal Security Program – Program Manual, November 2007

To locate these changes online—search on the date next to the revision bar. On the Adobe Reader toolbar, click Search. In the Search pane, type Nov 2007 and then click Search.

Change Summary	Description of Change	Where to Look
Title change	The title of the 'security best practices' manual has been changed to *POS Terminal Security Program – Security Guidelines*	Chapter 1
New evaluation laboratories	Brightsight (formerly TNO) and SecurityMetrics have been added to the list of PTS-approved laboratories.	Chapter 2
Device type withdrawn	The attribute 'Device Type' has been withdrawn.	Chapter 2
Model Name/Number	The use of a commercial Model Name/Number has been clarified in relation to the components that constitute the Platform Identifier.	Chapter 2
Hardware and Firmware details	The scope of Hardware and Firmware numbers has been clarified.	Chapter 2
Maintaining Approval	The procedures for maintaining the approval status for a modified platform have been clarified.	Chapter 2

MasterCard Worldwide

POS Terminal Security Program – Program Manual

November 2007

Proprietary Rights

Trademarks

Media

This document is available:

- On MasterCard OnLine®
- On the *MasterCard Electronic Library* (CD-ROM)

MasterCard Worldwide
2200 MasterCard Boulevard
O'Fallon MO 63368-7263
USA

1-636-722-6100

www.mastercard.com

Using this Manual

Chapter 1 Introduction

Chapter 2 Detailed Evaluation Process

Using this Manual

This chapter contains information that helps you understand and use this document.

Legal Terms and Conditions

Acceptance of the following terms and conditions is a condition of access to any information or data relating to the MasterCard POS Terminal Security Program (hereafter referred to as the "PTS Program") including, without limitation, that which is contained in this Program Manual.

No act or omission of MasterCard International Incorporated, its affiliates, or the agents, employees or contractors of any such party (together for the purposes of these legal terms and conditions, "MasterCard") in relation to the PTS Program, or issue of any certificate or approval under the PTS Program:

- Constitutes any guarantee, warranty, or endorsement of any product, whether express or implied. Without limitation, any implied warranties of merchantability, fitness for purpose, or non-infringement, are expressly disclaimed by MasterCard
- Is a guarantee of freedom from security vulnerabilities
- Constitutes any forward-looking statement but is instead limited to the circumstances prevailing at the time of such act or omission or the issue of any such certificate or approval

MasterCard:

- May amend, remove, add to or suspend any provision of the PTS Program, cease to operate the PTS Program in conjunction with any other party, or cease to operate the PTS Program, whether with or without replacing it with any other program, in its discretion and without notice
- Does not guarantee, warrant or endorse any products which are provided by any third party or which are subjected to the PTS Program

No vendor:

- May state, imply or infer that compliance with any aspect of the PTS Program is a warranty, endorsement, guarantee or recommendation of any product by MasterCard
- Shall have authority to make any statement to any third party that would constitute any implied or express endorsement or warranty regarding the functionality, quality or performance of any product or any aspect thereof by MasterCard

It shall be the sole responsibility of purchasers or issuers of any product:

- To obtain any warranties or other remedies in relation to such products from the vendors or other suppliers of such products
- To make their own checks, investigations and searches to ensure the functionality, security or fitness for purpose of any products

To the extent permitted by applicable law, MasterCard shall not be liable to any person having access to any information or data relating to the PTS Program, or any other third party (including such party's customers) for any loss, damages (including direct, special, punitive, exemplary, incidental or consequential damages) or costs (including attorneys' fees) which arise out of the performance or non-performance of any aspect of the PTS Program by MasterCard, or otherwise arise out of or are related to the PTS Program. The foregoing limitation of liability shall apply to any claim or cause of action under law or equity whatsoever, including contract, warranty, strict liability, or negligence, even if MasterCard has been notified of the possibility of such damages or claim.

These terms and conditions shall be governed by the laws of the State of New York, without regards to its conflict of laws provisions, and the parties submit to the exclusive jurisdiction of the federal and state courts located in the City and State of New York for the resolution of all matters relating to the PTS Program or these terms and conditions.

Purpose

The MasterCard *POS Terminal Security Program – Program Manual* describes the process of POS terminal evaluation and approval in the context of the MasterCard POS Terminal Security (PTS) Program.

The PTS program focuses on the evaluation of IP-enabled dedicated/stand-alone POS devices or mobile devices, used in acceptance environments that are exposed to the Internet or other public or wireless networks.

Audience

MasterCard provides this document primarily for platform vendors and manufacturers.

Overview

The following table provides an overview of this manual:

Chapter	Description
Table of Contents	A list of the manual's chapters and subsections. Each entry references a chapter and page number.
Using this Manual	A description of the manual's purpose and its contents.
1 Introduction	Provides an overview of the POS Terminal Security Program.
2 Detailed Evaluation Process	Provides operational details about the POS Terminal Security Program.

Language Use

The spelling of English words in this manual follows the convention used for U.S. English as defined in *Merriam-Webster's Collegiate Dictionary*. MasterCard is incorporated in the United States and publishes in the United States. Therefore, this publication uses U.S. English spelling and grammar rules.

An exception to the above spelling rule concerns the spelling of proper nouns. In this case, we use the local English spelling.

Times Expressed

MasterCard is a global company with locations in many time zones. The MasterCard operations and business centers are in the United States. The operations center is in St. Louis, Missouri, and the business center is in Purchase, New York.

For operational purposes, MasterCard refers to time frames in this manual as either "St. Louis time" or "New York time." Coordinated Universal Time (UTC) is the basis for measuring time throughout the world. You can use the following table to convert any time used in this manual into the correct time in another zone:

	St. Louis, Missouri USA Central Time	**Purchase, New York USA** Eastern Time	**UTC**
Standard time (first Sunday in November to second Sunday in March [a])	09:00	10:00	15:00
Daylight saving time (second Sunday in March to first Sunday in November)	09:00	10:00	14:00

[a] For Central European Time, last Sunday in October to last Sunday in March.

Revisions

MasterCard periodically will issue revisions to this document as we implement enhancements and changes, or as corrections are required.

With each revision, we include a "Summary of Changes" describing how the text changed. Revision markers (vertical lines in the right margin) indicate where the text changed. The month and year of the revision appear at the right of each revision marker.

MasterCard may publish revisions to this document in a MasterCard bulletin, another MasterCard publication, or on MasterCard OnLine. A subsequent revision is effective as of the date indicated in that publication or on MasterCard OnLine and has precedence over any previous edition. In the event of a conflict between this document and a subsequently published edition, the subsequently published edition shall have precedence.

Related Information

The following documents and resources provide information related to the subjects discussed in this manual. For descriptions of these documents, please refer to the List of Manuals in the Member Publications product on MasterCard OnLine®.

- *POS Terminal Security Program – Security Requirements*
- *POS Terminal Security Program – Derived Test Requirements*
- *POS Terminal Security Program – Vendor Questionnaire*
- *POS Terminal Security Program – Security Guidelines*
- *POS Terminal Security Program – SSL/TLS Implementation Guidelines*
- *POS Terminal Security Program – Approval List*

Nov 2007

Note **These documents are routinely updated and reaffirmed. The current versions should be referenced when using these requirements.**

Members that use the Cirrus® service and logo or that process online debit transactions should refer to the debit processing manuals recommended by the Customer Operations Services team.

Terminology

The following table provides definitions of the key terms used in this manual. For all other terms, please refer to the *MasterCard Dictionary* on the Member Publications home page (on MasterCard OnLine® and the MasterCard Electronic Library CD-ROM). You also may access the MasterCard Dictionary from the main menu and bookmark pane of most manuals.

Term	Definition
Cryptographic protocol	Set of rules and procedures that enable the interoperability of security processes. An example is TLS, which provides services like data confidentiality or peer authentication as part of the TCP/IP suite.
Cryptography algorithm	A cryptographic process used to achieve a specific secure service (for example confidentiality, through the algorithm 3DES).
Integrity	Ensuring consistency of data; in particular, preventing unauthorized and undetected creation, alteration, or destruction of data.
IP Protocols/Services	Generic designation of the set of open protocols and services used in the Internet. In the context of this document, the set includes IP Protocols (such as ICMP, UDP, or TCP), IP Security Protocols (such as SSL, IPSec, or PPTP) and IP Services (such as DHCP, HTTP, or FTP).
IP-enabled POS terminal	*See Platform*
Key management	The activities involving the handling of cryptographic keys and other related security parameters (e.g., initialization vectors, counters) during the entire life cycle of the keys, including their generation, storage, distribution, loading and use, deletion, destruction, and archiving.
Merchant	An entity that contracts with an acquirer to originate transactions and that displays card acceptance marks for financial transactions.
Platform	A POS device (or a subsystem of a POS device), subject to evaluation in the framework of the MasterCard POS Terminal Security Program. The platform provides to the application layers of a POS device the functionality and security related to IP Protocols/Services.

Term	Definition
POS device	Any device that participates in transaction processing at the point of sale (by processing, storing, or forwarding transaction, card, and cardholder data) and interfaces to a public communication network using Internet protocols (the TCP/IP suite of protocols).
POS Terminal Security Program	The MasterCard security evaluation program providing assurance to members that approved platforms meet the MasterCard POS Terminal Security Requirements.
Sensitive data (information)	Data which must be protected against unauthorized disclosure, alteration or destruction, especially plaintext PINs, and secret and private cryptographic keys, and includes design characteristics, status information, and so forth.
Session key	A key established by a key management protocol, which provides security services to data transferred between the parties. A single protocol execution may establish multiple session keys, e.g., an encryption key and a MAC key.

Support

Please address your questions to the Customer Operations Services team as follows:

Phone: 1-800-999-0363 or 1-636-722-6176

1-636-722-6292 (Spanish language support)

Fax: 1-636-722-7192

E-mail:

Canada, Caribbean, Latin America, South Asia/Middle East/Africa, and U.S.	customer_support@mastercard.com
Asia/Pacific:	
Australia and New Zealand	csd@mastercard.com
China, Hong Kong, and Taiwan	helpdesk.gc@mastercard.com
Southeast Asia	helpdesk.singapore@mastercard.com
Japan/Guam	opetokyo@mastercard.com
Korea	korea_helpdesk@mastercard.com
Europe	css@mastercard.com
Spanish language support	lagroup@mastercard.com
Vendor Relations, all regions	vendor.program@mastercard.com

Address: MasterCard Worldwide
Customer Operations Services
2200 MasterCard Boulevard
O'Fallon MO 63368-7263
USA

Telex: 434800 *answerback*: 434800 ITAC UI

Member Relations Representative

Member Relations representatives assist U.S. members with marketing inquiries. They interpret member requests and requirements, analyze them, and if approved, monitor their progress through the various MasterCard departments. This does not cover support for day-to-day operational problems, which the Customer Operations Services team addresses.

For the name of your U.S. Member Relations representative, contact your local Member Relations office:

Atlanta	1-678-459-9000
Chicago	1-847-375-4000
Purchase	1-914-249-2000
San Francisco	1-925-866-7700

Regional Representative

The regional representatives work out of the regional offices. Their role is to serve as intermediaries between the members and other departments in MasterCard. Members can inquire and receive responses in their own languages and during their offices' hours of operation.

For the name of the location of the regional office serving your area, call the Customer Operations Services team at:

Phone: 1-800-999-0363 or 1-636-722-6176

1-636-722-6292 (Spanish language support)

1 Introduction

This chapter provides an overview of the POS Terminal Security Program and describes the approval process.

Process Description

This chapter describes the procedures for submitting an IP-enabled POS terminal (platform) for evaluation in the context of the MasterCard POS Terminal Security (PTS) Program.

Throughout this manual, the term **platform** is used to refer to an IP-enabled POS device (or subsystem/peripheral of a POS device) that provides to the application layers of a POS device, functionality and security related to IP protocols and services.

Vendors must first contact one of the PTS-approved laboratories and complete the forms and questionnaires contained in the following documents:

- *POS Terminal Security Program – Security Requirements*
- *POS Terminal Security Program – Vendor Questionnaire*

The vendor then submits the platform for evaluation, together with any additional documentation required by the laboratory to support the testing process. Upon completion of the evaluation, MasterCard will review the laboratory's *Evaluation Report* to check for compliance with the requirements of the POS Terminal Security Program.

If the product meets MasterCard requirements, the product will be deemed to be 'approved' and the vendor will be issued with an *Approval Letter*, confirming successful completion of the process. MasterCard will also list the details of that platform on the MasterCard OnLine® Web site.

Process Flow

The following diagrams show the overall process flow in graphic form. The various actions and decisions are split between the vendor, the evaluation laboratory, and MasterCard.

Figure 1.1 shows the process for the evaluation and approval of a new platform.

Figure 1.2 shows the process for changes to an existing approved platform, and for the renewal of an existing platform approval. This process links back to Figure 1.1 at points 'A' and 'B', as shown.

Figure 1.1—Security Evaluation and Approval Process

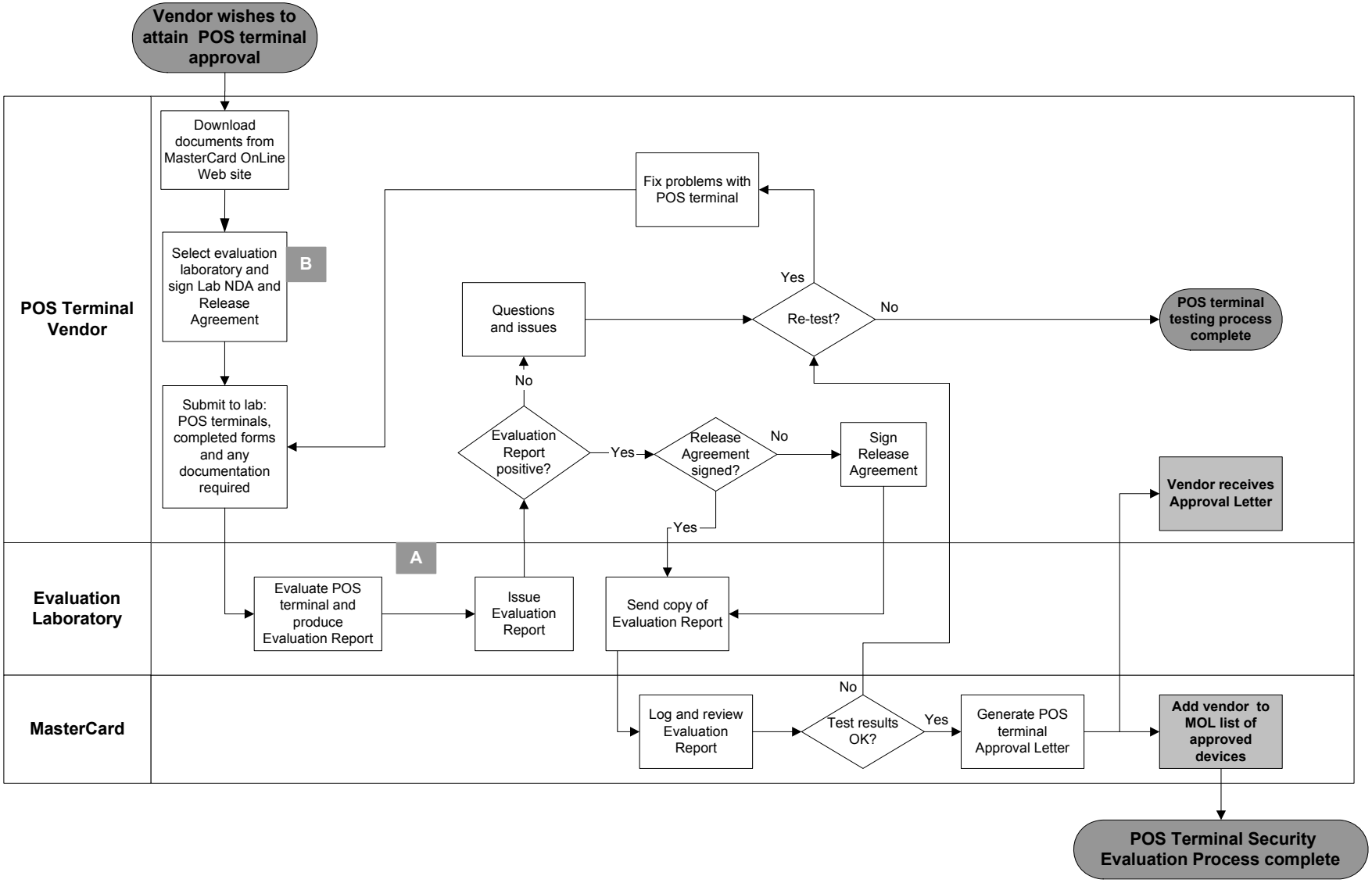
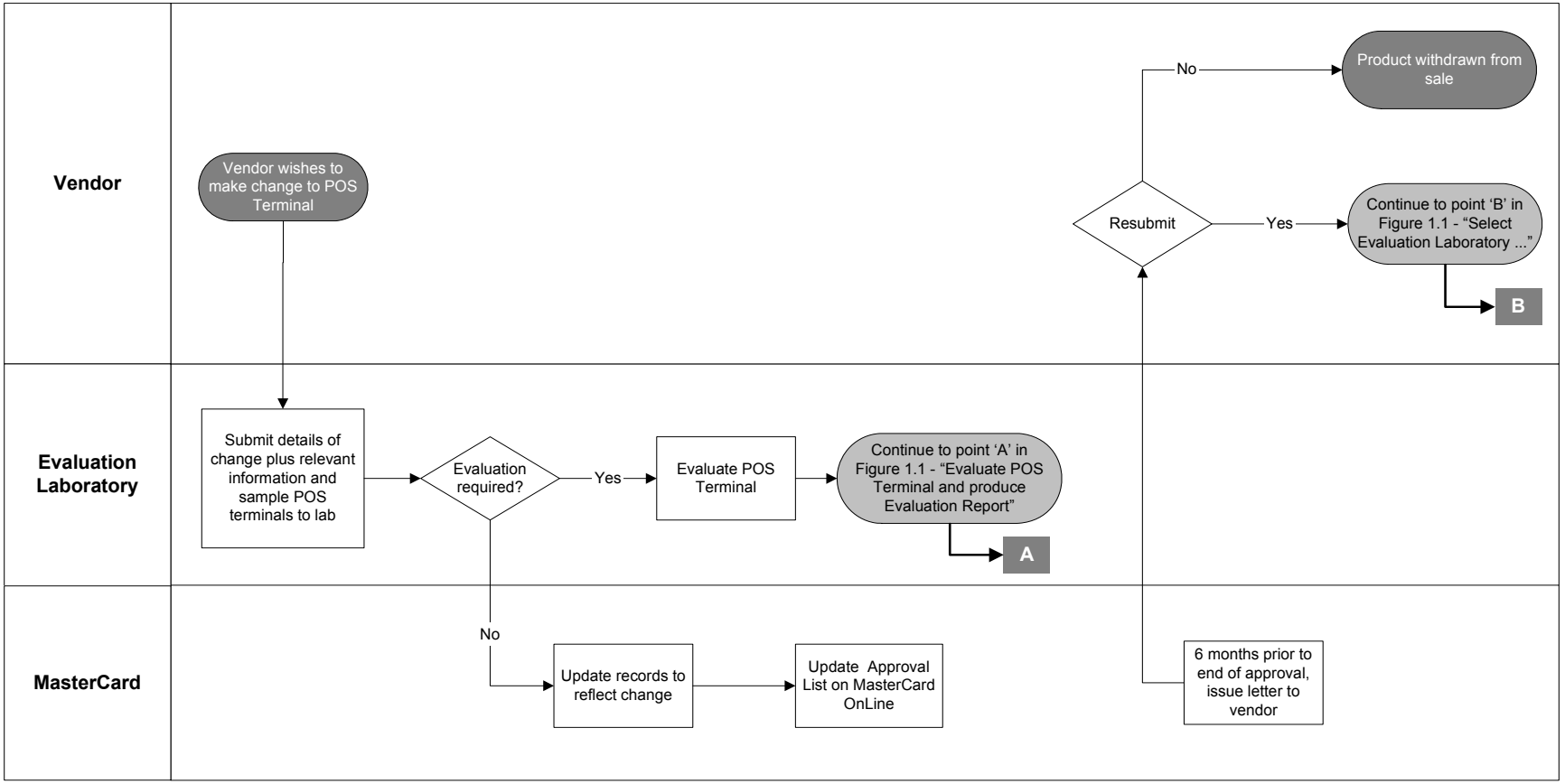


Figure 1.2—Security Evaluation – Change Request and Renewal Process



Documentation

Refer to the following documents for further information about the POS Terminal Security Program:

- *POS Terminal Security Program – Security Requirements*
- *POS Terminal Security Program – Vendor Questionnaire*
- *POS Terminal Security Program – Derived Test Requirements*
- *POS Terminal Security Program – Security Guidelines*
- *POS Terminal Security Program – SSL/TLS Implementation Guidelines*
- *POS Terminal Security Program – Approval List*

Nov 2007

All documents are available in electronic form on MasterCard OnLine.

Updates to Documents and Security Requirements

Security is a never-ending race against potential attackers. As a result, it is necessary to:

- Regularly review, update, and improve the security requirements for IP-enabled POS terminals.
- Periodically update the *POS Terminal Security Program – Security Requirements* manual and the related *POS Terminal Security Program – Derived Test Requirements* manual.

To make the introduction of new security requirements easier for vendors, MasterCard will publish updated manuals in advance of the actual implementation of new security requirements, and will clearly indicate an **effective date** for any new security requirements.

Note **MasterCard reserves the right to change, amend, or withdraw security requirements at any time. If such a change is required, MasterCard will endeavor to work closely with members and vendors to help reduce the impact of any changes.**

Contact Details

For further information about any aspect of the POS Terminal Security Program, please contact:

MasterCard PTS Program Coordinator:

Tel: +32 2 352 5782

Fax: +32 2 352 4999

E-mail: pts@mastercard.com

2 Detailed Evaluation Process

This chapter provides an overview of the POS Terminal Security Program and describes the approval process.

Introduction

From 1 April 2006, terminal platforms that are 'Internet Protocol (IP)' enabled may be evaluated against the security requirements defined in the *POS Terminal Security Program – Security Requirements* manual.

A PTS-approved evaluation laboratory will evaluate the vendor's compliance statements, information provided in a *Vendor Questionnaire*, along with product samples of the platform being evaluated.

The laboratory will subject the platform to various tests, as defined in the *POS Terminal Security Program – Derived Test Requirements* manual, and make judgments on the outcome of these tests.

Following evaluation, MasterCard will review the *Evaluation Report* issued by the laboratory. If the results are satisfactory, then the platform will be 'approved', and MasterCard will issue an *Approval Letter* to the vendor. MasterCard will then publish details of that approved platform on its MasterCard Online® Web site.

Required Documentation and Other Items

All information and documents relevant to the POS Terminal Security Program can be downloaded from the MasterCard OnLine Web site. Evaluation-specific information should be requested directly from the chosen laboratory.

Completed forms and questionnaires relating to platform evaluation must be delivered directly to one of the PTS-approved laboratories.

Vendors must submit the following documents and items to their chosen laboratory:

- Completed Security Compliance Statements from the *POS Terminal Security Program – Security Requirements* manual.
- Completed questionnaire from the *POS Terminal Security Program – Vendor Questionnaire* manual.
- Three (3) working POS terminals with Operator's Manual, or instructions.
- The necessary hardware and software accessories for the laboratory to assess the security of the platform's network interface, the robustness of the IP protocol implementation, and the use of IP authentication/ encryption protocols.
- Documentation and user guidance that describes the functions used by third-party application developers, system integrators, and other end-users.
- Documentation that relates to the security management of the platform.
- Instructions and accessories that will allow the test laboratory engineers to use all special modes that the platform supports, including key management and maintenance functions.
- Additional documentation, such as block diagrams, schematics, and flow charts that will assist in the evaluation of the platform (the laboratory may request additional evaluation material when necessary).

Following a successful evaluation, the vendor must provide MasterCard with two (2) platforms – identical to those evaluated by the PTS-approved laboratory.

MasterCard will securely retain these platforms, and may use them to assess or to develop new attack techniques. Also, if that platform was ever compromised in the field, the retained samples may be used to investigate any compromise or security breach.

Preparation for Testing

To facilitate the evaluation process prior to actual testing, PTS-approved laboratories may offer the following services to vendors:

- Provide guidance on designing platforms to security requirements.
- Review a vendor's platform design, answer questions via e-mail or phone, and participate in conference calls to clarify requirements.
- Provide guidance on bringing a vendor's platform into compliance with stated requirements if areas of non-compliance are identified during the evaluation.

Vendors are encouraged to contact a PTS-approved laboratory directly regarding the above services, and any associated fees.

Note **PTS-approved laboratories cannot perform the actual design of the platform.**

Approved Laboratories

Vendors may contact any of the following PTS-approved laboratories to obtain information about the services they offer, and to request advice and documentation on scheduling test dates, and about test fees:

Nov 2007

Brightsight (formerly TNO)

Contact: Rob van Marrewijk
E-mail: marrewijk@brightsight.com
Tel: +31 15 269 2522
Fax: +31 15 269 2555

EWA-Canada Ltd

Contact: Paul Zatychec or Steven Bowles
E-mail: pcilab@ewa-canada.com
Tel: +1 613 230 6067 (Extension 1227)
Fax: +1 613 230 4933

Infogard

Contact: Doug Biggs
E-mail: dbiggs@infogard.com
Tel: +1 805 783 0810

RFI Global Services Ltd

Contact: Barry Gilbert
E-mail: barry.gilbert@rfi-global.com
Tel: +44 1256 312081
Fax: +44 1256 312001

SecurityMetrics

Contact: PTS Department
E-mail: pts@securitymetrics.com
Tel: +1 801 705 5656
Fax: +1 801 724-9700

SRC Security Research & Consulting GmbH

Contact: Detlef Klaus
E-mail: detlef.kraus@src-gmbh.de
Tel: +49 228 2806 100
Fax: +49 228 2806 199

T-Systems

Contact: Robert Hammelrath
E-mail: robert.hammelrath@t-systems.com
Tel: +49 228 9841 114
Fax: +49 228 9841 60

Witham Laboratories

Contact: Stephen Roberts
E-mail: steve@withamlabs.com
Tel: +61 3 9846 2751
Fax: +61 3 9850 8866

Nov 2007

Fees

All laboratory evaluation fees (and dates) must be negotiated directly between the vendor and their selected laboratory.

MasterCard may, at its discretion, charge vendors an administrative fee to cover the costs involved in processing vendors' platform approvals.

Note **The vendor pays all laboratory evaluation fees directly to the laboratory.**

Requirements for Testing

As a requirement for testing, the platform vendor must complete the forms in the *POS Terminal Security Program – Security Requirements* manual along with the questionnaire contained in the *POS Terminal Security Program – Vendor Questionnaire*.

Vendors must submit all forms together with the necessary paperwork and product samples, directly to their chosen laboratory.

Note **The laboratory will review the responses provided in the various forms and supporting documentation, and may decide that the platform is not ready for evaluation until some corrective action has been taken.**

Testing Timeframes

Vendor should request information from the laboratory on when to start the actual evaluation, and its duration.

Timeslots must be scheduled in advance with the laboratory. Evaluations can be performed more quickly if the laboratory has all of the required documentation and hardware, and there are no significant compliance issues.

If problems are discovered during testing, discussions between the laboratory and the vendor may be required. Such discussions may impact testing times and cause delays, or end the test cycle prior to the completion of all tests.

Evaluation Vendor Support

The laboratory may, at its discretion, seek additional information from the vendor that may resolve any discrepancy found during the evaluation. If the discrepancy requires the vendor to modify the platform's firmware, then the vendor must submit the platform for re-evaluation, and the laboratory will invoice the vendor accordingly.

MasterCard recommends that vendors designate a technical person to be available to assist with any questions that may arise during laboratory testing. During the evaluation, and to expedite the process, this person should be 'on call' to discuss discrepancies and respond to questions from the laboratory.

Approval Process

MasterCard will only review platform evaluation reports delivered by the laboratory directly to MasterCard. MasterCard will not grant any 'partial approvals' based upon the ability of a platform to meet some – but not all – of the stated requirements.

Note

PTS-approved laboratories only perform platform testing and will generate an *Evaluation Report* based on their test results; they do not have any approval authority.

Only MasterCard has platform approval authority, and will base its approval solely on the results contained in the laboratory's *Evaluation Report*.

If the *Evaluation Report* indicates that all applicable security requirements have been met, then MasterCard will issue an approval for that platform.

A MasterCard approval, in the form of an *Approval Letter* and Web site listing, will provide at least the following information:

- Platform Identifier
- Approval Number
- Renewal Date

Nov 2007

Where an approved platform is integrated into some other device, the platform vendor may indicate the actual commercial designation of the end POS device(s).

The platform vendor is responsible for the accuracy of such information and the use of approved platforms within integrated POS devices.

Platform Identifier

Platforms submitted for testing must be properly identified so that members or their agents can be confident in purchasing IP-enabled platforms that have been approved by the MasterCard POS Terminal Security Program.

MasterCard uses the **Platform Identifier** to denote all relevant information, which is representative of an approved platform. The Platform Identifier consists of:

- Hardware #
- Firmware #
- Application # (if applicable)

Nov 2007

Note **The 'Model Name/Number' is the commercial name used to identify one or more POS devices based on the platform. It does not belong to the set of components that constitute the Platform Identifier.**

Nov 2007

By associating a particular Model Name/Number with the Platform Identifier, a vendor's customers can easily associate the approved platform with the commercial names of POS devices based on that platform.

The Platform Identifier will be included in the *Approval Letter* and in the *POS Terminal Security Program – Approval List* published on MasterCard OnLine.

To ensure that a particular platform has received an approval, acquiring members or their designated agents are strongly advised to purchase and deploy only those platform models where the information matches exactly the designations given in the components of the Platform Identifier.

Table 2.1—Example of a Platform Identifier used by a Family of POS Terminals

Nov 2007

Component	Example Description
Hardware #:	NN-421-000-AB
Firmware #:	Ver. 1.01
Applic. #:	4.5.3

Hardware # and Firmware

Nov 2007

The combination of the Firmware and Application version numbers must encompass all communication-related software, including drivers, Operating System, core IP layers, protocols, and services.

The fields that make up the Hardware # and Firmware # may consist of a combination of fixed and variable alphanumeric characters. A lower case 'x' is used to designate variable fields. The 'x' represents fields that the vendor can change at any time to denote a different platform configuration, for example, country usage code, customer code, etc.

The 'x' field(s) will have been assessed – by both the evaluation laboratory and MasterCard – as to not impact the platform's security requirements or the vendor's approval. To ensure that the platform has been approved, acquiring members or their designated agents are strongly advised to purchase and deploy only those platforms where the fixed alphanumeric characters of the Hardware # and Firmware # match **exactly** those stated in the *POS Terminal Security Program – Approval List*, or in the vendor's *Approval Letter* from MasterCard. Platform vendors may have produced platforms with the same Model Name/Number (prior to validation of compliance by the laboratory) that do not meet with MasterCard security requirements.

If an identical platform is used across a family of devices, vendors are cautioned against assigning a Hardware # or Firmware # that might restrict approval only to one particular model of terminal.

Nov 2007

Renewal Date

Approvals are valid for **three (3) years,** starting from the published date of the platform's *Evaluation Report* delivered to MasterCard by the laboratory.

If an approved platform has undergone changes that may potentially affect its security, or if the vendor wants the components of the Platform Identifier revised (in its *Approval Letter* and on MasterCard OnLine), then the vendor must submit proper change documentation to the laboratory in order for it to determine whether further evaluation is required. Refer to Changes to a Previously Approved Platform for details.

Nov 2007

The laboratory will communicate to MasterCard any information relating to changes that may affect a previously approved platform. MasterCard will acknowledge these updates in the form of a revised *Approval Letter* and Web site listing. However, in such cases, the platform's approval expiry date will remain the same.

Note **If platform vendors can modularize the platform's functionality, it would help to minimize re-evaluations due to changes that do not impact platform security.**

Requesting an Approval

Vendors are required to sign a *MasterCard Release Agreement* form which, among other things, will allow the laboratory to release the *Evaluation Report* to MasterCard for approval consideration.

Upon receipt of a positive *Evaluation Report* from the laboratory, MasterCard will issue an *Approval Letter*, and post details of the approved platform model on the MasterCard OnLine Web site within thirty (30) days.

Refer to Figure 1.1 in Chapter 1 for process details.

Approval Renewal Process

Approximately six (6) months before the platform's approval is due to expire, the PTS Program Coordinator will contact the vendor to determine whether the vendor intends to renew the platform's approval. At this point, there are two options for the vendor to consider:

- Allow MasterCard to remove the platform's details from the *POS Terminal Security Program – Approval List* after the due expiry date, or
- Contact the PTS-approved laboratory and submit details of any modifications made since the laboratory last reviewed the platform, or its change documents.

With the second option, the laboratory will determine whether the platform needs to undergo a full re-evaluation against the current PTS security requirements, and notify the vendor accordingly.

Upon receipt from the laboratory of either a successful test report, or a letter stating that any changes made to the platform do not affect security, and that the platform is in compliance with the most recent version of the PTS security requirements, MasterCard will then extend the platform's approval for another three (3) years.

Refer to Figure 1.2 in Chapter 1 for process details.

Changes to a Previously Approved Platform

Although subject to continual refinements, the following applies when changes are made to a previously approved platform. Refer to Figure 1.2 in Chapter 1 for process details.

Maintaining Approval

The following scenarios are possible:

a) New Testing is Not Required to Maintain Approval

Nov 2007

1. If the hardware or firmware in the previously approved platform is revised then documentation of the change must be submitted to a laboratory for review (it is strongly recommended that the vendor uses the same PTS-approved laboratory as was used for the original evaluation). Where appropriate, the laboratory will issue a letter to MasterCard describing the nature of the change, stating that it does not impact compliance with the PTS security requirements. MasterCard will then review the letter to determine whether the change has any impact to the approval status of the platform.

   Assuming no impact then the platform, as identified by its Platform Identifier, would be considered 'Approved'. MasterCard will then issue an updated *Approval Letter* to the vendor, and update the platform's details in the *POS Terminal Security Program – Approval List*, as published on MasterCard OnLine.

2. If the hardware or firmware in the previously approved platform is revised and changes do not affect security, the vendor need not submit documentation of the change to the laboratory, unless requested by MasterCard. The vendor's internal change management process must document the changes made to the approved platform, and this documentation must be made available promptly to MasterCard on request.

b) New Testing is Required to Maintain Approval

If changes to the platform do impact security, then the product must undergo another security evaluation. The laboratory will then submit a new *Evaluation Report* to MasterCard, for re-approval consideration.

(In this scenario, the vendor must first submit documentation of the change to the laboratory, which will determine whether the nature of the change impacts platform security in accordance with the current PTS security requirements.)

Boundary of Approval

The process by which an approval of an existing platform can be carried over to a new (or similar) platform is as follows:

a. Vendor describes the design of the new (or similar) platform in the form of a **revision document** and sends this to the selected laboratory for review.

b. Laboratory reviews the documentation (and possibly platform samples).

c. Laboratory treats the document review process like a revision of an existing approved platform.

d. Laboratory then sends a letter to the vendor stating whether a full test evaluation is required, or not.

Notification Following a Security Breach or Compromise

Vendors must notify MasterCard of any security breach or compromise that occurs in relation to an approved platform, using the procedures described in this section.

Notification and Timing

Not withstanding any other legal obligations the vendor may have, the vendor must immediately notify MasterCard of any security breach or compromise relating to any:

- Approved platform(s)
- Platform development process
- Manufacturing facility

The vendor must also provide immediate feedback to MasterCard about any potential impact this (possible or actual) breach may or will have on MasterCard, its members, or merchants.

Note **Notification must take place no later than 24 hours after the vendor first discovers the security breach or compromise.**

Notification Format

The vendor's initial notification of a security breach or compromise must take the form of a phone call to the MasterCard PTS Program Coordinator, followed by an e-mail, Fax, or letter providing full details of the security breach or compromise.

Refer to Chapter 1 for contact details.

Notification Details

Following notification of a security breach or compromise, the vendor must supply the PTS Program Coordinator with all relevant information relating to that security breach or compromise. This will include, but is not limited to:

- The number and location of actual products affected
- The number of compromised accounts (if known)
- Details of any compromised keys
- Any reports detailing the security breach or compromise
- Any reports or evaluations performed to investigate the security breach or compromise

MasterCard, as agreed within the terms of the *MasterCard Release Agreement*, may share this information with PTS-approved laboratories to enable an evaluation of the security breach or compromise to be performed in order to mitigate or prevent further security breaches or compromises.

As a result of this notification, MasterCard will work with the vendor to correct any security weaknesses, and will produce a guideline document – to be issued to that vendor's customers, informing them of any potential vulnerability, and detailing what actions should be taken in order to mitigate or prevent further security breaches or compromises.

Actions following a Security Breach or Compromise

In the event of MasterCard being made aware of a security weakness or actual compromise related to a specific platform, or group of platforms, as listed in the *POS Terminal Security Program – Approval List*, then MasterCard will take the following actions:

- Attempt to obtain the compromised platform to evaluate exactly how the compromise occurred. This may include utilizing PTS-approved laboratories.
- Contact the vendor to inform them that their product has a security weakness, or has been compromised and, where possible, share information relating to the actual weakness or compromise.
- Work with the vendor to try and mitigate or prevent further compromises.
- Work with appropriate law enforcement agencies to help mitigate or prevent further compromises.
- Perform evaluations on the compromised platform either internally or under the terms of the *MasterCard Release Agreement* using PTS-approved laboratories, in order to identify the cause of the compromise.
- Follow internal escalation procedures, as appropriate.

Once all investigations into the security breach or compromise have been completed, MasterCard in consultation with the vendor will:

- Issue a *Security Bulletin* detailing the security weakness or compromise, utilizing as little confidential information as possible.
- Generate a *Guidelines Document*, to be issued to merchants and members, detailing 'best practices' to be followed in order to mitigate the associated security risk or compromise.

If cooperation between MasterCard and the vendor cannot be reached then MasterCard will issue a *Security Bulletin* informing members of a security weakness or compromise associated with a particular vendor and advising the members to contact the vendor for further information.

MasterCard will also share details of the compromise with all PTS-approved laboratories so that details of how the compromise occurred can be taken into account for future PTS Program security evaluations.

Withdrawal of Approval

MasterCard reserves the right to withdraw a platform's approval and remove that platform from the *POS Terminal Security Program – Approval List*, when it is clear that the platform does not offer sufficient protection against current threats, and does not conform to PTS security requirements.

If MasterCard considers that the platform has a security weakness or has been compromised, then MasterCard will notify the vendor, in writing, of its intent to withdraw its approval of that platform.

Fourteen days after issuing the letter of intent, MasterCard will remove the details of that platform from the *POS Terminal Security Program – Approval List*.

Appeal Against Withdrawal

After receipt of an 'intent to withdraw' notification from MasterCard, the vendor may appeal against such withdrawal. MasterCard must receive any appeal (in writing) within 14 days of the original notification being issued.

An appeal meeting will be arranged between MasterCard and the vendor, and any other parties MasterCard may wish to invite. The agenda of the meeting will be strictly limited to the security breach or compromise as it relates to the vendor's product.

If the outcome of the appeal is successful then the platform will remain on the list of approved platforms.

If the appeal is unsuccessful, MasterCard will remove that platform from the *POS Terminal Security Program – Approval List*.

Activities after Withdrawal and Waiver Process

Removal of a platform from the *POS Terminal Security Program – Approval List* does not affect those platforms that are already deployed. However, the vendor in conjunction with MasterCard must produce a guideline document to be issued by the vendor to all its customers. The purpose of such a document is to help to mitigate or prevent any further compromises.

Acquirers that wish to continue to deploy a vendor's platform after its approval has been withdrawn must first contact MasterCard to request a waiver, using the standard MasterCard waiver process.

Regaining Product Approval Status

If a vendor wishes to regain PTS Program approval for a platform that has had its approval withdrawn by MasterCard, then the vendor must:

- Correct any weaknesses identified during the assessment of the compromised platform.
- Ensure that the **Platform Identifier** is clearly changed between the original compromised platform and the revised platform being submitted for approval.
- Submit samples (and related documentation) to a PTS-approved laboratory for security evaluation against the current *POS Terminal Security Program – Security Requirements*.

Upon successful completion of the evaluation, the platform will again be listed as an 'approved' platform – but under its new Platform Identifier.