

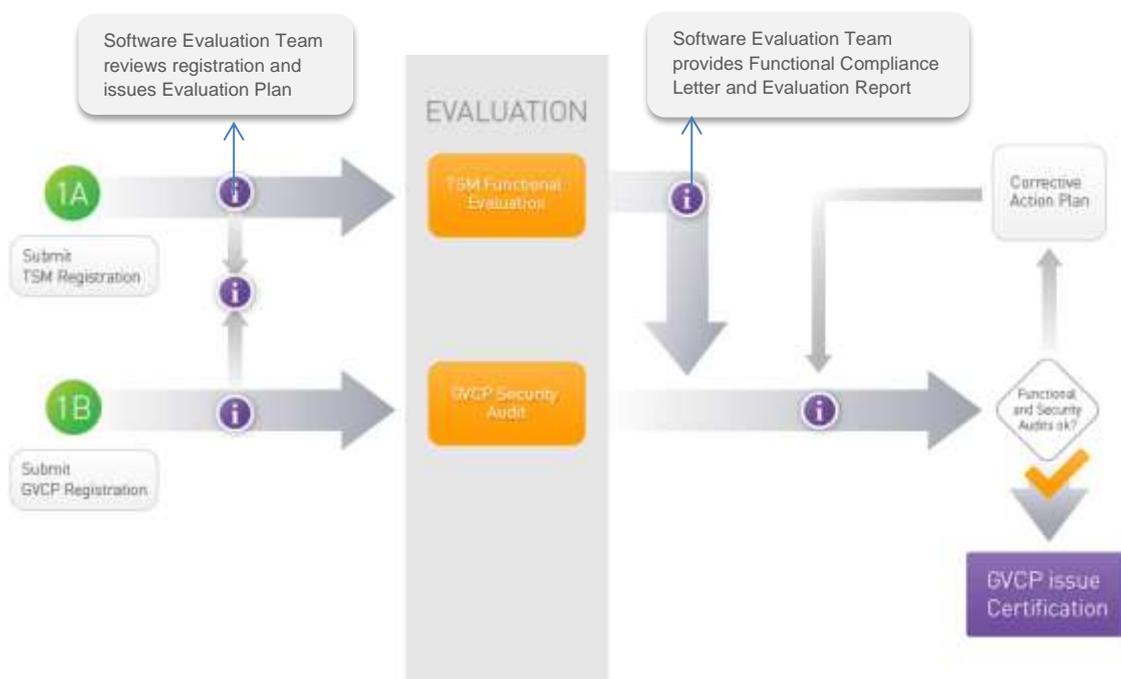
MasterCard TSM Approval Fact Sheet

February 2015 - Version 2.0

TSM Approval Process Overview

The MasterCard TSM Approval process relates to the approval of Trusted Service Managers (TSM) that provide Over-The-Air (OTA) provisioning services to deploy MasterCard Payment Applications and cardholder data to secure elements within mobile devices. The approval process has the following two streams that can be initiated in parallel as shown below:

1. TSM Functional Approval Process
2. Site Security Assessment using Global Vendor Certification Program (GVCP)



1. TSM Functional Approval Process

The TSM Functional Approval process is managed by the Software Evaluations team at MasterCard. The TSM evaluation looks at the functional roles of the TSM System, the functions supported by the TSM Platform it is based on, and checks them against MasterCard TSM Functional Requirements. If all TSM Functional Requirements are successfully met, the Software Evaluations Team will issue a “Functional Compliance Letter” indicating that the TSM system based on a specific TSM Platform and in a specific configuration is functionally compliant, and can be deployed at a MasterCard Approved Secure facility. The GVCP Process will require the Functional Compliance Letter in order to issue the final GVCP certificate for a particular site installation.

2. Site Security Assessment using GVCP

The Global Vendor Certification Program (GVCP) requires all third-party vendors such as card manufacturers, card personalization bureaus and TSM vendors, among others to comply with GVCP Requirements. In relation to TSMs, GVCP requires a security audit of the facility where the

TSM System is hosted. The audit looks at physical, logical and procedural security. If the GVCP audit results are successful and the TSM system has received a Functional Compliance Letter, the GVCP help desk will issue a certificate for “Over-the-Air (OTA)” provisioning. Please contact GVCP-helpdesk@mastercard.com for details of how to register for the program.

Note: *GVCP involves legal agreements and annual fees that apply. Also, because this program requires audits by independent external auditors, you are advised to begin this process at the earliest opportunity to avoid delays.*

TSM Documents

Documents associated with the TSM approval process can be found on the MasterCard Mobile Partner website at the following address: www.mastercard-mobilepartner.com

- MasterCard TSM Functional Requirements, Feb 2015 – Version 2.0
- MasterCard TSM Approval Guide, May 2015 – Version 2.0

GVCP Documents

After contacting and registering with the GVCP help desk, you will receive a package of documentation including security standards and requirements documents, a fees schedule, accredited audit firms, agreement documents etc.

Detailed Steps in the TSM Functional Approval process

The first step of the process is to register the TSM for approval. This is done by completing the TSM registration form and submitting it to Software_Evaluations@mastercard.com

The Software Evaluations team will then send an Evaluation plan to you, stating the conditions of the evaluation. In general the evaluation process consists of three steps.

1. TSM Platform evaluation - You will be asked to fill an evaluation script to determine the level of compliance of the TSM Platform against a set of TSM functional requirements. The TSM Platform evaluation can be skipped if it is already approved in other configurations.
2. TSM System evaluation - You will be asked to provide a document or presentation describing the SE hierarchy (before and after provision), key exchange between TSMs and functional workflows on the configuration of the TSM System. This will form the basis for discussion during the evaluation.
3. TSM Demonstration - This is a demonstration of the TSM System in operation (test data can be used. Live keys etc. are not necessary). Certain use cases will be evaluated, supported either with recorded video and/or server messaging logs.

Upon completion of the evaluation, the Software Evaluations Team will send you a Functional Compliance Letter or and Evaluation Completion Letter along with an Evaluation Report.

Throughout the process, support is available from:
Software Evaluations Team
Software_evaluations@mastercard.com

GVCP Team
GVCP-helpdesk@mastercard.com

Frequently Asked Questions (FAQ)

Since TSM systems are complex, the following FAQ section is written in general terms. All TSM systems are assessed and evaluated on a case by case basis.

FAQ 1 – Why is there a TSM Approval Process?

It is primarily to help protect the MasterCard brand and Issuer brand, and to provide a level of confidence that the TSM System meets certain basic capabilities that are required by the market. The approvals process does this by checking that the TSM System complies with requirements that protect the MasterCard payment application and cardholder data.

FAQ 2 – What does MasterCard consider as TSM?

If your system does any of the following, it is considered to be a TSM.

1. Life cycle management of Secure Element.
Such as managing the Secure Element Life Cycle states during pre-issuance and post-issuance of the Secure Element. (Provided by SEI TSMs)
2. Life cycle management of Security Domains on the Secure Element.
Such as providing secured blocks of space in the Secure Element for services. (Normally provided by SEI TSMs)
3. Life cycle management of executable load-files/applets on the Security Domain of a Secure Element.
Such as downloading of executable load-files, installation, extradition and deletion of the applets. (Can be provided by SEI TSMs but also SP TSMs)
4. Mobile payment application personalization.
Such as preparation and personalization of card holder data and card data in to the mobile payment application. (Normally provided by SP TSMs)
5. Post-issuance mobile payment application management.
Such as issuer scripting via over the air communications to the mobile payment application. (Normally provided by SP TSMs)

Where,

- SEI TSM is a Secure Element Issuer TSM that is run by the SE Issuer to manage the Secure Element.
- SP TSM is a Service Provider TSM which is a third-party system connecting the Issuing bank to the Secure Element Issuer.

FAQ 3 – Does the approval process apply to SEI TSM and SP TSM?

The approvals process is mainly concerned with SP TSMs. SEI TSMs are generally out of scope for TSM approval except when they:

- Have access to personalization data, secret financial keys or post-issuance application management scripts directly.
- Can access to personalization data, secret financial keys or post-issuance application management scripts via decryption with known keys.

- Are capable of personalization and post-issuance of EMV scripts to the MasterCard payment application in the secure element (point 4 and 5 in FAQ 2).

FAQ 4 - When must the TSM approval process be applied?

You need to apply for TSM approval if your TSM System performs point 4 and/or 5 in FAQ 2.

FAQ 5 – As a TSM vendor, do I need to sign a licensing agreement?

You need to sign a MasterCard M/Chip Mobile License Agreement if your TSM System needs TSM approval. If you are a SEI TSM and manage the life cycle of MasterCard Payment Application (see point 3 in FAQ 2), you do not need TSM approval, but then you are still required to sign a MasterCard M/Chip License Agreement.

Vendors who do not yet have a relevant license agreement in place should contact the Software Evaluations team at Software_Evaluations@mastercard.com.

FAQ 6 – I am a MasterCard Issuer and I’m going to host my own TSM, do I need approval?

Because you are a MasterCard Issuer you can host and run a TSM System for your own issuance at your own risk, and you do not need TSM approval. TSM approval is needed if you plan to offer TSM services to other parties.

FAQ 7 – Are there any hardware requirements?

The TSM software may run on any operating system and there are no specific requirements for the computers used. But GVCP has requirements for Cryptographic Security Modules (i.e. HSMs) and requirements around how the system is networked.

FAQ 8 – Can my TSM be hosted at a data center or be cloud-based?

Generally data centers that offer high availability operation are not normally designed to meet banking security standards. The GVCP requirements involve high levels of physical, logical and procedural security which means that the TSM System cannot be hosted in areas where other operations are carried out. Personnel that have access to the TSM System must also be tightly controlled. There might also be legal implications, since the company registering the TSM System must be responsible for its security and operation. This could be difficult to achieve because there would be two legal entities involved, the TSM owner and the hosting facility owner.

FAQ 9 – Will you test my TSM System?

No, the evaluation process only looks at Self-Assessment Questionnaires and supporting documents (workflows and SE content diagram and may include messaging logs from the configured TSM System). MasterCard does not test the system or its interfaces.

FAQ 10 – I am a TSM software vendor and intend to sell the software, can I get certified?

It is not possible to give certification to the TSM software without it being hosted in a secure facility. This is because the certification combines the functional evaluation with the GVCP security audit of the hosting facility. It may be possible to go through the functional evaluation of the TSM software, but a certificate will not be issued.

FAQ 11 – How much does the TSM approval process cost?

At this time (Feb 2015) there is no fee for TSM functional evaluation. Although, please note that GVCP charges license fees and costs will be incurred during the independent audit process.

FAQ 12 – How long will the TSM Functional evaluations take?

Typically, you will receive an evaluation plan within 5 working days of acceptance of your TSM registration document. Once the necessary documentation has been received by MasterCard, the evaluation can begin. The functional evaluation takes about a day to complete. Expect to receive results within 10 working days after the evaluation.

FAQ 13 – How long will the GVCP certification process take?

Because of the use of independent auditors, you should allow a minimum of three months for the completion of the GVCP certification process.