# Certification Report

## Verifone MX 9x5 Payment Terminal

| | |
|---|---|
| Sponsor and developer: | ***Verifone (UK) Ltd***<br>**Symphony House,7 Cowley Business Park, High Street**<br>**Cowley, Uxbridge, UB8 2AD**<br>**United Kingdom** |
| Evaluation facility: | ***Brightsight***<br>**Delftechpark 1**<br>**2628 XJ Delft**<br>**The Netherlands** |
| Report number: | **NSCIB-CC-11-33074-CR** |
| Report version: | **1** |
| Project number: | **NSCIB-CC-11-33074** |
| Authors(s): | **Denise Cater** |
| Date: | **September 30, 2014** |
| Number of pages: | **14** |
| Number of appendices: | **0** |

*Reproduction of this report is authorized provided the report is reproduced in its entirety.*

Head office Apeldoorn:
Boogschutterstraat 11A
P.O. Box 541
7300 AM Apeldoorn
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

Location Apeldoorn:
Vissenstraat 6
P.O. Box 541
7300 AM Apeldoorn
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

Location Enschede:
Josink Esweg 10
P.O. Box 337
7500 AH Enschede
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 859

TÜV Rheinland Nederland B.V. is a
registered company with the
Amsterdam Chamber of Commerce
under number 27288788
info@nl.tuv.com
www.tuv.com/nl

# Certificate

Standard

Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 3 (ISO/IEC 15408)

Certificate number **C11-33074**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer

## Verifone (UK) Ltd

**Symphony House,7 Cowley Business Park, High Street**
**Cowley, Uxbridge, UB8 2AD United Kingdom**

Product and assurance level

**Verifone MX 9x5 Payment Terminal,**

Assurance Package:

- EAL POI

Protection Profile Conformance:

- ANSSI-CC-PP-2010/10: Point of Interaction Protection Profile ANSSI-CC-PP-POI-COMPREHENSIVE, Date: 26 November, 2010 Version: 2.0

Project number **NSCIB-CC-11-33074-CR**

Evaluation facility **Brightsight BV located in Delft, the Netherlands**

Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 3 (ISO/IEC 18045)

Common Criteria Recognition Arrangement for components up to EAL4

SOGIS IT SECURITY CERTIFIED

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 3 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 3. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Validity

Date of issue : **06-10-2014**
Certificate expiry : **06-10-2019**

Registration number
PRODUCTS
RvA C078
Accredited by the Dutch Council for Accreditation

TÜV Rheinland Nederland B.V.
P.O. Box 541
7300 AM Apeldoorn
The Netherlands

TÜVRheinland®
Precisely Right.

# CONTENTS:

**Foreword** 4

**Recognition of the certificate** 5

**1 Executive Summary** 6

**2 Certification Results** 7

2.1 Identification of Target of Evaluation 7
2.2 Security Policy 7
2.3 Assumptions and Clarification of Scope 8
2.4 Architectural Information 9
2.5 Documentation 10
2.6 IT Product Testing 10
2.7 Evaluated Configuration 11
2.8 Results of the Evaluation 11
2.9 Evaluator Comments/Recommendations 12

**3 Security Target** 13

**4 Definitions** 13

**5 Bibliography** 14

# Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products.

A part of the procedure is the technical examination (evaluation) of the product according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a license is accreditation to the requirements of ISO Standard 17025, General requirements for the accreditation of calibration and testing laboratories.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

## Recognition of the certificate

The Common Criteria Recognition Arrangement and SOG-IS logos are printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.

# 1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Verifone MX 9x5 Payment Terminal. The developer of the Verifone MX 9x5 Payment Terminal is Verifone (UK) Ltd located in Uxbridge, UK and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE is a payment terminal with Integrated Circuit (IC) Card based online and offline payment transaction capabilities. The TOE is a Point-of-Interaction (POI) that manages payment transaction data and provides external communications capabilities excluding applications. The TOE consists of a PED (PIN Entry Device) with PIN keypad, display and a hybrid IC (Integrated Circuit) and Magnetic Stripe Card Reader.

The TOE includes security features used by payment applications, but the payment applications themselves are not part of the TOE. Any other part of the MX 9x5 like other functionalities than payment, which might be processed by the MX 9x5, e.g. fleet card processing, are also out of scope of the TOE and thus out of scope of the Security Target. The usage of the name POI in the following addresses the whole MX 9x5. If only a subset of the MX 9x5 is addressed, TOE or PED or any other logical or physical component name is used.

There are two models for the TOE: MX 915 and MX 925. All security features of these two models are the same. The only difference is that the MX 925 has 4.3” Display and Touch Panel; and MX 915 has 7” display and Touch Panel.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands and was completed on September 15 2014 with the delivery of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*. The certification was completed on September 17 2014 with the preparation of this Certification Report. It should be noted that the certification results only apply to the specific version of the product as evaluated.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the Verifone MX 9x5 Payment Terminal, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the Verifone MX 9x5 Payment Terminal are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]*[1] for this product provide sufficient evidence that it meets the EAL POI assurance requirements, as defined in *[PP]*, for the evaluated security functionality.

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3 *[CEM]*, for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 3 *[CC]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the Verifone MX 9x5 Payment Terminal evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. It should be noted that the certification results only apply to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

# 2 Certification Results

## 2.1 *Identification of Target of Evaluation*

The Target of Evaluation (TOE) for this evaluation is the Verifone MX 9x5 Payment Terminal from Verifone (UK) Ltd located in Uxbridge, UK.

The TOE is comprised of the following main components:

| Delivery item type | Identifier | Version |
|---|---|---|
| Hardware | VeriFone MX 915 or | P132-409-01-R |
| | VeriFone MX 925 | P132-509-01-R |
| Software | Vault | 5.6.1 |
| | Application Manager | 5.0.0 |
| | SRED | 4.1.78 |
| | OP | 4.0.0 |
| | Linux | 2.6.31 |
| Manuals | Mx900 series Installation guide<br>SPC132-022-01-A | Rev A |
| | Mx900 series Programmers guide<br>SPC132-021-01-A | Rev 1B |
| | Mx900 series Reference Manual<br>SPC132-020-01-A | Rev A |
| | Mx900 series VRK Payload Installation Guide<br>SPC132-034-01-A | Rev A |

To ensure secure usage a set of guidance documents is provided together with the Verifone MX 9x5 Payment Terminal. Details can be found in section 2.5 of this report.

## 2.2 *Security Policy*

The major security features provided by the TOE are detailed in the SFR packages defined in [PP] and summarized as follows:

- PIN Entry without exposure of PIN digits.
- Encipherment of PIN for offline or online Cardholder encrypted PIN authentication and transfer for further processing (to the IC Card Reader or to the Acquirer).
- Protected transmission of PIN for offline Cardholder authentication of Plaintext PIN to the IC Card Reader. Applicable only to integrated architectures where PED and IC Card Reader are enclosed into one tamper-responsive boundary.
- Periodic authentication of PIN processing software.
- Authenticity and integrity protection of administration (e.g. downloading, update) of PIN processing software and keys, including appropriate cryptographic means.

- Integrity protection of POI management and payment transaction data and cryptographic means to protect payment transaction data at external communication lines against disclosure and modification.
- Authenticity and integrity protection of administration (e.g. downloading, update) of POI management and transaction processing software and keys, including appropriate cryptographic means.
- Control of PED prompts.
- Tamper-detection/tamper-responsive (PED, PED SM, IC Card Reader, Magnetic Stripe Reader).
- Secure downloading of payment application.

## *2.3 Assumptions and Clarification of Scope*

### 2.3.1 Usage assumptions

The TOE is contained within a tamper responsive boundary requiring minimal usage assumptions regarding the operation for the TOE by users:

- Cardholders shall be asked to keep the PIN secret and not to hand their IC cards to other persons than a trustworthy merchant

### 2.3.2 Environmental assumptions

The following assumptions apply in the environment in which the TOE is deployed:

- The payment application providers have chosen appropriate security measures to protect devices interacting with the TOE e.g. the IC or Magnetic Stripe cards.
- User PINs as well as the IC Cards are securely managed by the Issuer. Especially it is assumed that the PIN as well as IC Card transfer between Issuer and Cardholder takes place in a manner that the confidentially of the PINs is ensured and the misuse of the cards is prevented by organisational measures.

Furthermore, the following organisational security policy relates to the environment in which the TOE shall be operated (for the detailed and precise definition of the organisational security policy refer to the *[ST]*, chapter 4.5):

- OSP.WellFormedPayApp detailing the Payment Application(s) shall use the security mechanisms provided by the TOE to protect the assets.
- OSP.ApplicationSeparation detailing the separation of applications if the TOE provides a multiple application environment.
- OSP.POISurvey detailing procedural measures to be taken to inspect the TOE enclosure for signs of tampering.
- OSP.MerchantSurvey detailing the merchant responsibilities to inspect the interfaces in the TOE enclosure and the payment schemes to detect manipulations are large numbers of payment transactions.
- OSP.KeyManagement detailing procedural measures to securely manage the generation and installation of cryptographic keys and certificates.

### 2.3.3 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

The TOE consists in the whole MX 9X5 excluding applications. However, the IC Contactless Reader, the Capacitive Touch Display, the communications modules do not interfere with the security features of the TOE and either provide only functional communication capabilities or are components used by non-payment applications.

## 2.4 Architectural Information

The MX 9X5 is a multipurpose payment system built on the Linux operating system. Developers can create applications for new and existing merchants. The MX 9X5 provides multiple connectivity and communication options to support solutions for onsite repair persons, taxi drivers, kiosk vendors, on casino floors and more.

The MX 9X5 provides an LCD colour touch screen for cardholder interaction. When used in low lighting conditions, the MX 9X5 provides additional illumination at the card reader and keypad areas for cardholder convenience. The MX 9X5 is ideally suited for mobile merchants who want to take payments directly to the cardholder for secure card authentication and PIN entry.

The physical security of the MX 9X5 has been designed in compliance with the security requirements of [PP]. The MX 9X5 contains multiple tamper mechanisms and a secure microcontroller, mitigating malicious attempts to gain access to sensitive data.

- Physical Design / Layout: The physical design methodology is to protect all sensitive data in a centralized location inside the MX 9X5. Attacks on this location cause noticeable tamper evidence, activates a tamper event, or causes irreparable damage.
- By case switches, keypad removal switches, usage of a security controller, security cover and tamper-circuits the MX 9X5 resists physical manipulation and manipulation of the hardware to protect the confidentiality of PINs and cryptographic keys including changing or monitoring environmental conditions.
- Multiple Tamper Mechanisms: The MX 9X5 employs multiple tamper mechanisms, allowing for security redundancy and robustness. The tamper mechanisms employed by the device protect against:
  - Penetration attempts
  - Separation of the cases halves
  - Separation of the keypad from the main PCB
  - Access to sensitive components; e.g. the keypad circuitry, secure microcontroller, external memory and IC Card Reader
  - Access to sensitive data; e.g. PIN data, cryptographic keys
  - Environmental and operational attacks
  - The device employs multiple logical security features:

The device employs multiple logical security features:

- Boot-up Process: This boot-up process is performed every time the TOE powers up.
- Selftests: The device performs a selftest when it starts up as well as at least once every 24 hours.
- Logical anomalies: The device mitigates against logical anomalies. A distinct API with acceptable parameters is used to ensure correct functionality.
- Download: Keys, firmware, application and prompts are successfully downloaded if and only if they are authentic. Asymmetric techniques are used to ensure authenticity. In addition secret keys are protected against disclosure.
- PIN digit display: The TOE outputs non-specific characters to the display in lieu of PIN digits.
- Buffers processing: All buffers are cleared as soon as possible.
- Sensitive services: Key loading, firmware and application/prompt loading are the only two sensitive services utilized by the TOE.
- The TOE provides a random number generator.
- The TOE supports Master Key / Session Key as well as DUKPT as key management techniques for online PIN encryption.
- Cryptographic keys are only used for their intended purpose.
- Cryptographic keys are protected against disclosure.

- The procedure for PIN entry is distinct and exclusive of any other data capture functionality.
- Application processing payment transactions are separated from other applications.
- Authenticity and integrity of POI management and transaction data.

## *2.5 Documentation*

The following documentation is provided with the product by the developer to the customer:

| Identifier | Version |
|---|---|
| Mx900 series Installation guide SPC132-022-01-A | Rev A |
| Mx900 series Programmers guide SPC132-021-01-A | Rev 1B |
| Mx900 series Programmers guide SPC132-021-01-A | Rev A |
| Mx900 series VRK Payload Installation Guide SPC132-034-01-A | Rev A |

## *2.6 IT Product Testing*

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer’s testing activities documentation and verified that the developer has met their testing responsibilities.

### 2.6.1 Testing approach and depth

The developer performed at least one test case to demonstrate the behaviour of each TSFI, with the exception of the SAM slots. Therefore an evaluator test case was added to test the SAM slot.

The evaluator repeated a sample (>50%) of the developer test cases. The sample of test cases selected by the evaluator cover all security functions. A total of 11 independent functional test cases and 7 developer test cases were repeated by the evaluator.

Evaluator and developer test cases were executed use one of two configurations:

- Production configuration (the certified configuration, as per the [ST])
- Development configuration (this is as for the certified configuration, together with the telnet port open for console access, which was required to support some of the test cases)

The final developer testing (executing all developer test cases) was performed on the version of hardware and software specified in [ST].

The evaluator testing was performed on a version of hardware (M132-509-11-R) which differed from the TOE version of the MX915 (P132-509-01R) only in relation to the security irrelevant CTLS. The software used during evaluator testing was as specified in [ST], with the exception of the Vault and Application Manager software components. These components were updated following evaluator testing. The evaluators performed source code analysis of the changes between the version tested and the final version, and determined the changes would not impact the test results obtained, as the changes were made to components that are not related to the provision of the SFRs.

### 2.6.2 Independent Penetration Testing

A total of 9 penetration test cases were executed by the evaluator. This included testing of the tamper responsive enclosure of the TOE.

### 2.6.3 Test Configuration

As detailed in Section 2.6.1 above, the evaluator and developer test cases were executed using one of two configurations:

- Production configuration (the certified configuration, as per the [ST])
- Development configuration (this is as for the certified configuration, together with the telnet port open for console access, which was required to support some of the test cases)

### 2.6.4 Testing Results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its ST and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

## *2.7 Evaluated Configuration*

The TOE is defined uniquely by its name "Verifone MX 9x5" and part/version numbers of the hardware and software components, as defined in Section 2.1 above. It should be noted that the hardware is labelled with two identifiers, which are identical except for the first position ("M" or "P"). The [ST] uses the PCI ID to uniquely identify the TOE, namely "P132-409-01-R" and "P132-509-01-R". The software component version numbers are displayed to the user during the power-on sequence of the TOE.

## *2.8 Results of the Evaluation*

The evaluation lab documented their evaluation results in the *[ETR]*[2] which references the ASE Intermediate Report and other [NSP#6] evaluator reports. The verdict of each claimed assurance requirement is given in the following tables:

| **Development** | | **Pass** |
|---|---|---|
| Security architecture | ADV_ARC.1 (refined) | Pass |
| Functional specification | ADV_FSP.2 | Pass |
| TOE design | ADV_TDS.1 | Pass |

| **Guidance documents** | | **Pass** |
|---|---|---|
| Operational user guidance | AGD_OPE.1 (refined) | Pass |
| Preparative procedures | AGD_PRE.1 | Pass |

| **Life-cycle support** | | **Pass** |
|---|---|---|
| Configuration Management capabilities | ALC_CMC.2 (refined) | Pass |
| Configuration Management scope | ALC_CMS.2 (refined) | Pass |
| Delivery | ALC_DEL.1 (refined) | Pass |
| Development security | ALC_DVS.2 (refined) | Pass |

| **Security Target** | | **Pass** |
|---|---|---|
| Conformance claims | ASE_CCL.1 | Pass |
| Extended components definition | ASE_ECD.1 | Pass |
| ST introduction | ASE_INT.1 | Pass |
| Security objectives | ASE_OBJ.2 | Pass |
| Security requirements | ASE_REQ.2 | Pass |

[2] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

| | | |
|---|---|---|
| Security problem definition | ASE_SPD.1 | Pass |
| TOE summary specification | ASE_TSS.1 | Pass |

| **Tests** | | **Pass** |
|---|---|---|
| Coverage | ATE_COV.1 | Pass |
| Functional tests | ATE_FUN.1 | Pass |
| Independent testing | ATE_IND.2 | Pass |

| **Vulnerability assessment** | | **Pass** |
|---|---|---|
| POI-Basic attack potential | AVA_POI.1/<br>MSR | Pass |
| POI-Low attack potential | AVA_POI.2/<br>PEDMiddleTSF | Pass |
| POI Low attack potential | AVA_POI.2/<br>MiddleTSF | Pass |
| POI Moderate attack potential | AVA_POI.3/<br>CoreTSF | Pass |
| POI High attack potential | AVA_POI.4/<br>CoreTSFKeys | Pass |

Based on the above evaluation results the evaluation lab concluded the Verifone MX 9x5 Payment Terminal, to be **CC Part 2 extended, CC Part 3 extended**, and to meet the requirements of **EAL POI**, as defined in *[PP]*. This implies that the product satisfies the security technical requirements specified in Security Target 'Security Target Verifone MX 9x5 Payment Terminal', SPC132-041-01-A, revision A06.

The Security Target claims conformance to the Point of Interaction Protection, 26 November, 2010, Version 2.0, registered and certified by ANSSI under the reference, ANSSI-CC-PP-2010/10.

## *2.9 Evaluator Comments/Recommendations*

### 2.9.1 Obligations and hints for the developer

The payment application developer must apply the guidance provided in "Mx900 Series Programmers Guide" [PG], in particular:

- Ensuring that the buffers used by the application processor are cleared
- Ensuring that no sensitive application data/application library are put under /home/usr*/lib folder.

It should be noted that the "Revision 1B" identifier of the "Mx900 Series Programmers Guide" is only indicated in the filename and revision table of the document [PG] (not on the front page).

### 2.9.2 Recommendations and hints for the customer

The User Guidance (as outlined in Section 2.5 of this report) contains necessary information about the usage of the TOE. In particular, the procedures detailed in the "Mx900 Series Installation Guide" [IG] and "Mx900 series Reference Manual", [RM] relating to the inspection of the interfaces and enclosure of the TOE must be applied to ensure the TOE is not modified or replaced.

# 3 Security Target

The ‘Security Target Verifone MX 9x5 Payment Terminal’, SPC132-041-01-A, Revision A06 is included here by reference. Please note that for the need of publication a public version ‘Security Target Verifone MX 9x5 Payment Terminal’, SPC132-043-01-A, Revision A03 has been created and verified according to *[ST-SAN]*.

# 4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

| | |
|---|---|
| ANSSI | L’Agence Nationale de la Sécurité des Systèmes d’Information |
| CTLS | Constrained Total Least-Squares |
| IC | Integrated Circuit |
| IT | Information Technology |
| ITSEF | IT Security Evaluation Facility |
| LCD | Liquid Crystal Display |
| MSR | Magnetic Stripe Reader |
| NSCIB | Nederlands Schema voor Certificatie op het gebied van IT-Beveiliging |
| PCB | Printed Circuit Board |
| PED | PIN Entry device |
| PIN | Personal Identiication Number |
| POI | Point Of Interaction |
| PP | Protection Profile |
| SFR | Security Functional Requirement |
| SM | Security Module |
| TOE | Target of Evaluation |
| TSF | TOE Security Functionality |

# 5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

[CC] Common Criteria for Information Technology Security Evaluation, Parts I, II and III, version 3.1, Revision 3, July 2009.

[CEM] Common Methodology for Information Technology Security Evaluation, version 3.1, Revision 3, July 2009.

[ETR] Brightsight, Evaluation Technical Report VeriFone MX 9x5 Payment Terminal EAL POI, 13-RPT-339, Version 7.0, 15 September 2014.

[IG] Mx900 series Installation guide, SPC132-022-01-A, Rev A

[NSCIB] Nederlands Schema voor Certificatie op het gebied van IT-Beveiliging, Version 2.0, 1 July 2011.

[NSP#6] NSCIB Scheme Procedure #6, Alternative Evaluator Reporting, Version 1.0, June 1st, 2012

[PG] Mx900 series Programmers guide, SPC132-021-01-A, Rev 1B

[PP] Point of Interaction Protection Profile ANSSI-CC-PP-POI-COMPREHENSIVE, Date: 26 November, 2010 Version: 2.0

[RM] Mx900 series Reference Manual, SPC132-020-01-A, Rev A

[ST] ‘Security Target Verifone MX 9x5 Payment Terminal’, SPC132-041-01-A, A06, 26 March 2014.

[STLite] ‘Security Target Verifone MX 9x5 Payment Terminal’, SPC132-043-01-A, A03, 11 September 2014.

[ST-SAN] ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.

[VPIG] Mx900 series VRK Payload Installation Guide, SPC132-034-01-A, Rev A

(This is the end of this report).