0122

Common Criteria Certification Report

No. CRP293

SCR200/SKP200

Version

	SCR200	SKP200
Software Version	• DPSSCR200 v1.3.0.8A • GridMonitor_SCR200 v1.037 • MagHead_SCR200 v1.02 • SBOOT v2.6	• DPSSKP200 v1.3.0.1A • GridMonitor_SKP200 v1.040 • SBOOT v2.6
Hardware Version	SCR200 version D	SKP200 version B

Issue 1.0

September 2016

CESG Certification Body
IA Service Management, CESG
Hubble Road, Cheltenham
Gloucestershire, GL51 0EX
United Kingdom

CERTIFICATION STATEMENT

The product detailed below has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme ('the Scheme') and has met the specified Common Criteria (CC) requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this Certification Report.

Sponsor	Payment Express Ltd.	Developer	Payment Express Ltd.
Product Name, Version		SCR200	SKP200
	Software Version	• DPSSCR200 v1.3.0.8A • GridMonitor_SCR200 v1.037 • MagHead_SCR200 v1.02 • SBOOT v2.6	• DPSSKP200 v1.3.0.1A • GridMonitor_SKP200 v1.040 • SBOOT v2.6
	Hardware Version	SCR200 version D	SKP200 version B
Platform/Integrated Circuit			
Description	Unattended payment terminal with a non-integrated structure, designed to be integrated into a kiosk, vending machine, fuel dispenser or similar devices.		
CC Version	Version 3.1 Release 4		
CC Part 2	Extended	CC Part 3	Extended
PP(s) or (c)PP Conformance	Point of Interaction Protection Profile Version 2.0, 26th Nov 2010 [PP]		
EAL	EAL POI, equivalent to CC EAL 2 augmented by ALC_DVS.2 and extended with AVA_POI		
CLEF	UL Transaction Security		
CC Certificate	P293	Date Certified	13 September 2016

The evaluation was performed in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in UK Scheme Publication 01 [UKSP01] and 02 [UKSP01]. The Scheme has established the CESG Certification Body, which is managed by CESG on behalf of Her Majesty's Government.

The purpose of the evaluation was to provide assurance about the effectiveness of the Target of Evaluation [TOE] in meeting its Security Target [ST], which prospective consumers are advised to read. To ensure that the ST gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against that baseline. Both parts of the evaluation were performed in accordance with Protection Profile [PP] and supporting documents [JIL], CC Parts 1, 2 and 3 [CC], the Common Evaluation Methodology [CEM] and relevant Interpretations.

The issuing of a Certification Report is a confirmation that the evaluation process has been performed properly and that no *exploitable* vulnerabilities have been found in the evaluated configuration of the TOE. It is not an endorsement of the product.

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES
IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY (CCRA)

The CESG Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement [CCRA] and, as such, this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements[1] contained in the certificate and in this Certification Report are those of the Qualified Certification Body which issued them and of the Evaluation Facility which performed the evaluation. There is no implication of acceptance by other Members of the Arrangement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed by a third party upon those judgements.

SENIOR OFFICIALS GROUP – INFORMATION SYSTEMS SECURITY (SOGIS)
MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES (MRA)

The SOGIS MRA logo which appears below confirms that the conformant certificate has been authorised by a Participant to the above Agreement [MRA] and it is the Participant's statement that the certificate has been issued in accordance with the terms of this Agreement.

The judgments[1] contained in the certificate and this Certification Report are those of the compliant Certification Body which issued them and of the Evaluation Facility which performed the evaluation. Use of the logo does not imply acceptance by other Participants of liability in respect of those judgments or for loss sustained as a result of reliance placed upon those judgments by a third party.

Common Criteria ®

SOGIS IT SECURITY CERTIFIED

[1] All judgements contained in this Certification Report, are covered by CCRA [CCRA] recognition for components up to EAL 2 only, i.e. the augmentation ALC_DVS.2 and AVA_POI extensions are not covered by the CCRA.
All judgements in this Certification Report are covered by the SOGIS MRA [MRA].

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of the above product at the stated version, to the Sponsor as summarised on Page 2 ‘Certification Statement’ of this report, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

2. Prospective consumers of the above product at the stated version should understand the specific scope of the certification by reading this report in conjunction with the Security Target [ST], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

3. The following products completed evaluation to EAL POI, equivalent to CC EAL 2 augmented by ALC_DVS.2 and extended with AVA_POI on 13 September 2016:

SCR200/SKP200

	SCR200	**SKP200**
Software Version	• **DPSSCR200 v1.3.0.8A** • **GridMonitor_SCR200 v1.037** • **MagHead_SCR200 v1.02** • **SBOOT v2.6**	• **DPSSKP200 v1.3.0.1A** • **GridMonitor_SKP200 v1.040** • **SBOOT v2.6**
Hardware Version	**SCR200 version D**	**SKP200 version B**

4. The Developer was Payment Express Limited.

5. The Target of Evaluation (TOE) contains two separate devices, a pinpad (SKP200) with integrated display and a secure card reader (SRC200) with both magnetic and IC card readers. The devices are connected together with a single serial cable, and the card reader is connected to a ‘system controller’ (not part of the TOE) with a separate serial cable. The TOE is intended for unattended use.

6. The evaluated configuration of this product is described in this report as the TOE. Details of the TOE Scope, its assumed environment and the evaluated configuration are given in Chapter III ‘Evaluation Configuration’ of this report.

7. The TOE provides a physical keypad, Magnetic Stripe Reader (MSR), Integrated Circuit Reader (ICCR), LCD display, and serial communications. The TOE includes two separate devices, a PINpad with integrated display (SKP200), and a secure card reader with both magnetic and IC card readers (SCR200). The devices are connected together with a single serial cable, and

the card reader is connected to a 'system controller' with a separate serial cable. **The system controller is outside the scope of the evaluation**.

8. An overview of the TOE and its product architecture can be found in Chapter IV 'TOE Architecture' of this report. Configuration requirements are specified in [ST, Section 2.2].

Protection Profile Conformance

9. The Security Target [ST] is certified as achieving conformance to the following protection profile:

    - Point of Interaction Protection Profile Version: 2.0, 26th November 2010 [PP]

10. The ST also includes security objectives, security assurance requirements and Security Functional Requirements (SFRs) additional to those of the Protection Profile.

    - None

Security Target

11. The Security Target [ST] fully specifies the TOE's Security Objectives, the Threats / Organisational Security Policies (OSPs) which these Objectives counter / meet and the SFRs that refine the Objectives. All of the SFRs are taken from [PP] which, in turn, are taken from CC Part 2 [CC2], except the extended SFRs FCS_RND, FIA_API and FPT_EMSEC; use of this standard facilitates comparison with other evaluated products.

12. The assurance requirements are taken from CC Part 3 [CC3], except AVA_POI.

13. The TOE security policies are detailed in [ST, Section 8.1] The OSPs that must be met are specified in [ST, Section 6.2].

14. The environmental objectives and assumptions related to the operating environment are detailed in Chapter III (in 'Environmental Requirements') of this report.

Cryptographic Mechanisms

15. The TDES, RSA and HMAC cryptographic mechanism contained in the TOE used for PIN encryption, Mutual authentication during key exchange and Firmware integrity checking are publicly known and as such it is the policy of CESG, as the UK National Technical Authority for cryptographic mechanisms, not to comment on its appropriateness or strength. However, the Evaluators confirmed its correct implementation.

Evaluation Conduct

16. The methodology described in [CEM_POI] has been used to conduct the evaluation and the [CEM] for the evaluation activities not covered by

[CEM_POI]. The TOE is a Point of Interaction (POI) product type, so additional supporting documentation related to the Joint Interpretation Library (JIL) has been used. The applied documentation is the following:

- JIL CEM refinements for POI Evaluation [CEM_POI].
- JIL attack methods [JIL_AM] and attack potential [JIL_AP] for POIs.

17. As the TOE is a POI product (POI-COMPREHENSIVE configuration) the evaluation was performed against the Point of Interaction Protection Profile [PP].

18. The vulnerability assessment approach for this evaluation adopted the definition in the Protection Profile [PP]. CESG notes that a newer definition is described in version 4.0 of the Protection Profile. The evaluation was conducted using the latest known attack methods and state of the art equipment at the time of evaluation.

19. A source code review has been performed for both SKP200 and SCR200 units of the TOE with the objective of verifying the actual firmware implementation of those parts that enforce the SFRs and to check the overall software implementation looking for potential weaknesses (buffer overflow, command injection, etc.) and the presence of hidden or undocumented functionalities or commands.

20. An on-site audit was performed to the facilities where the TOE final assembly and initial key loading phases are carried out.

21. The developer provided samples specifically modified to ease the side channel and fault injection tests, under control of the evaluators.

22. The evaluation used CCRA supporting documents (as appropriate) and international interpretations, including SOGIS supporting documents defined in [JIL].

23. The CESG Certification Body monitored the evaluation, which was performed by the UL Transaction Security Commercial Evaluation Facility (CLEF). The evaluation addressed the requirements specified in the Security Target [ST]. The results of this work, completed in March 2016, were reported in the Evaluation Technical Report [ETR].

Evaluated Configuration

24. The TOE should be used in accordance with the environmental assumptions specified in the Security Target [ST]. Prospective consumers are advised to check that the SFRs and the evaluated configuration match their identified requirements, and to give due consideration to the recommendations and caveats of this report.

25. The TOE should be used in accordance with its supporting guidance documentation included in the evaluated configuration.

Conclusions

26. The conclusions of the CESG Certification Body are summarised on page 2 ‘Certification Statement’ of this report.

Recommendations

27. Chapter II ‘TOE Security Guidance’ of this report includes a number of recommendations regarding the secure delivery, receipt, installation, configuration and operation of the TOE.

28. Any further recommendations are included in the TOE Security Guidance in Chapter II, paragraph 41.

Disclaimers

29. This Certification Report and associated Certificate applies only to the specific version of the product in its evaluated configuration (i.e. the TOE). This is specified in Chapter III ‘Evaluation Configuration’ of this report. The ETR on which this Certification Report is based relates only to the specific items tested.

30. Certification is *not* a guarantee of freedom from security vulnerabilities. There remains a small probability that exploitable vulnerabilities may be discovered after the Evaluators’ penetration tests were completed. This report reflects the CESG Certification Body’s view on that date (see paragraph 77).

31. Existing and prospective consumers should check regularly for themselves whether any security vulnerabilities have been discovered since the date of the penetration tests (as detailed in Chapter V) and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether those patches have further assurance.

32. The installation of patches for security vulnerabilities, whether or not those patches have further assurance, should improve the security of the TOE but should only be applied in accordance with a consumer’s risk management policy. However, note that unevaluated patching will invalidate the certification of the TOE, unless the TOE has undergone a formal recertification or is covered under an approved Assurance Continuity process by a CCRA certificate authorising Scheme.

33. All product or company names used in this report are for identification purposes only and may be trademarks of their respective owners.

34. Note that the opinions and interpretations stated in this report under ‘Recommendations’ and ‘TOE Security Guidance’ are based on the experience of the CESG Certification Body in performing similar work under the Scheme.

II. TOE SECURITY GUIDANCE

Introduction

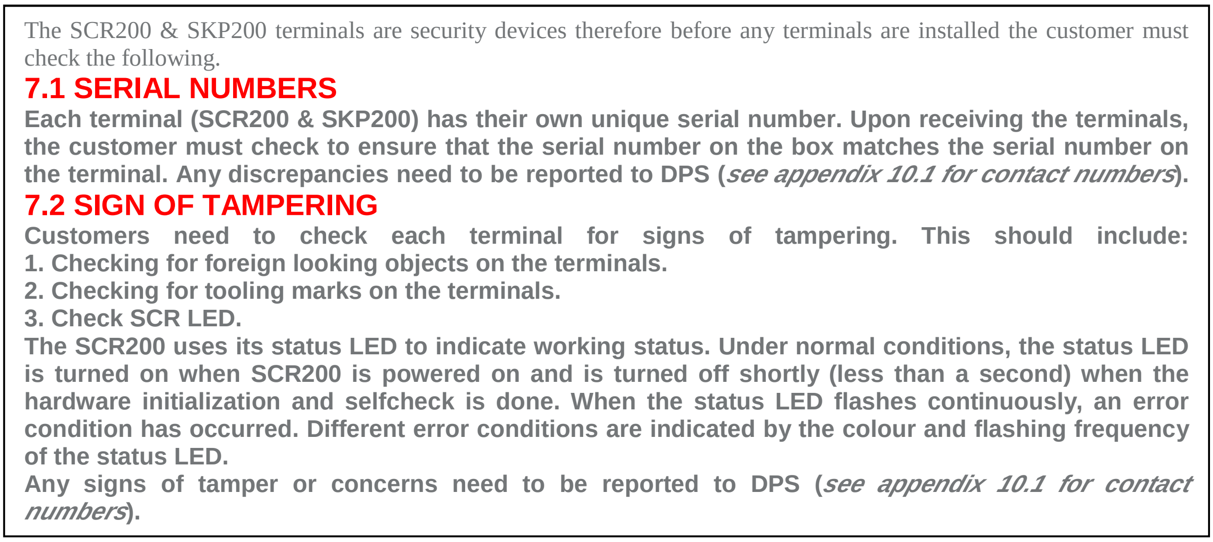
35. The following sections provide guidance that is of particular relevance to consumers of the TOE.

Delivery and Installation

36. On receipt of the TOE, the consumer should check that the evaluated version has been supplied, and should check that the security of the TOE has not been compromised during delivery. Specific advice on delivery and installation is provided in the TOE document(s) detailed below:

- Section 7 of Administration Guide [AG]

37. In particular, Users and Administrators should note that …



The SCR200 & SKP200 terminals are security devices therefore before any terminals are installed the customer must check the following.

7.1 SERIAL NUMBERS

Each terminal (SCR200 & SKP200) has their own unique serial number. Upon receiving the terminals, the customer must check to ensure that the serial number on the box matches the serial number on the terminal. Any discrepancies need to be reported to DPS (*see appendix 10.1 for contact numbers*).

7.2 SIGN OF TAMPERING

Customers need to check each terminal for signs of tampering. This should include:
1. Checking for foreign looking objects on the terminals.
2. Checking for tooling marks on the terminals.
3. Check SCR LED.
The SCR200 uses its status LED to indicate working status. Under normal conditions, the status LED is turned on when SCR200 is powered on and is turned off shortly (less than a second) when the hardware initialization and selfcheck is done. When the status LED flashes continuously, an error condition has occurred. Different error conditions are indicated by the colour and flashing frequency of the status LED.
Any signs of tamper or concerns need to be reported to DPS (*see appendix 10.1 for contact numbers*).

Guidance Documents

38. Specific configuration advice is in the Secure Configuration documents below:

- Not Applicable

39. The User Guide and Administration Guide documentation is as follows:

- Administration Guide [AG]
- Developer’s Guide [DG1]
- Developer’s Guide [DG2]

40. To maintain secure operation, the consumer is recommended to follow the security directives as detailed in [AG].

Recommendations

41. No additional recommendations.

III. EVALUATED CONFIGURATION

TOE Identification

42. The TOE is

SCR200/SKP200

	SCR200	SKP200
Software Version	• DPSSCR200 v1.3.0.8A • GridMonitor_SCR200 v1.037 • MagHead_SCR200 v1.02 • SBOOT v2.6	• DPSSKP200 v1.3.0.1A • GridMonitor_SKP200 v1.040 • SBOOT v2.6
Hardware Version	SCR200 version D	SKP200 version B

which consists of two separate units: the PIN entry device (SKP200) and the card reader (SCR200). Both units share a common software structure based on a secure bootloader (that replaces the processor manufacturer bootstrap), the monolithic firmware and a specific firmware (running on a separate processor) monitoring the tamper detection countermeasures.

TOE Documentation

43. The relevant guidance documents for the evaluated configuration are identified in Chapter II (in ‘Guidance Documents') of this report.

TOE Scope

44. The TOE Scope is defined in [ST, Section 2.2]. Functionality that is outside the TOE Scope is defined in [ST, Sections 2.5 and 1.2.2].

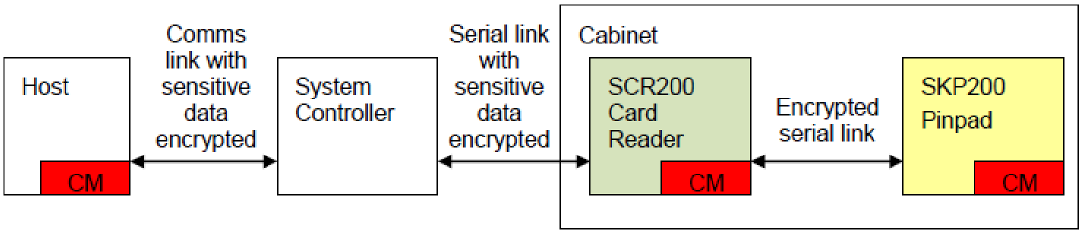
45. All parts of the product are in scope of the TOE, except the optional privacy shielding. The product is connected only to the System Controller, which is not part of the TOE nor in scope of the evaluation.

TOE Configuration

46. The evaluated configurations of the TOE are defined in [ST, Sections 2.1 - 2.2].

47. The TOE is a product of type POI in configuration POI-COMPREHENSIVE, providing protection for both IC and Magnetic Stripe card based transactions. It provides payment transaction data management and external communication facilities for interaction with the Acquirer.

48. The TOE provides a physical keypad, MSR, ICCR, LCD display, and serial communications. The TOE includes two separate devices, a PINpad with integrated display (SKP200), and a secure card reader with both magnetic and IC card readers (SCR200). The devices are connected together with a single serial cable, and the card reader is connected to a ‘system controller’ with a separate serial cable. The system controller is outside the scope of the evaluation.



Environmental Requirements

49. The environmental objectives for the TOE are stated in [ST, Section 5.2].

50. The environmental assumptions for the TOE are stated in [ST, Section 4.6].

51. The TOE is a monolithic product, not designed to run on top of any platform.

52. The environmental IT configuration is:

- The TOE requires an IT infrastructure able to transport messages from/to the system controller and the TOE (a single serial channel) for transaction processing.
- The TOE requires an IT infrastructure able to provide transaction data, e.g. amount, and to control the transaction flow.

Test Configurations

53. The Developers used this configuration for their testing:

- The Developer has run their regression test on samples configured as defined in paragraph 42.

54. The Evaluators used this configuration for their testing:

- The evaluators have conducted the testing on samples configured as defined in paragraph 42, with the exception of DFA and side channel testing, that required specially crafted samples, and hardware penetration tests not related to the firmware version.

IV. TOE ARCHITECTURE

Introduction

55. This Chapter gives an overview of the product and the TOE’s main architectural features. Other details of the scope of evaluation are given in Chapter III ‘Evaluated Configuration’ of this report.

56. The TOE contains two separate devices, a pinpad (SKP200) with integrated display and a secure card reader (SRC200) with both magnetic and IC card readers. The devices are connected together with a single serial cable, and the card reader is connected to a ‘system controller’ (not part of the TOE) with a separate serial cable.

57. The TOE provides the following security features:

- PIN management, for both online and offline PIN
- Magnetic stripe reader with protection of the cardholder data
- ICC reader with protection of the ICC plaintext PIN and cardholder data
- Display with protection of prompt during non-PIN data entry
- Secured keyboard with anti-tampering countermeasures
- Secure container with anti-tampering countermeasures, causing an automatic erasure of TOE secret keys upon activation
- Secure channel for communication to the remote server
- Secure channel for sensitive information exchange between the two components of the TOE
- Integrity and authenticity checking of the installed firmware and further updates.

TOE Description and Architecture

58. The TOE is made of two separate units: the PIN entry device (SKP200) and the card reader (SCR200). Both units share a common hardware and software structure.

59. The hardware is built around an Atmel AT91SO51 processor. This processor contains 32Kbytes of ROM, used for the bootstrap module, and 256Kbytes of EEPROM, used for storing vendor developed code. The hardware also includes a Texas Instruments MSP430F233 low power microcontroller that continuously monitors the tamper detection countermeasures, even in power down state. The secure processors and other security components are enclosed secure volume built with pcbs having anti-penetration wire meshes and closing pcb fences. Additionally, the SCR200 includes a third processor (STMicroelectronics, STM32F101) in charge of reading and encryption of magnetic stripe cards.

60. The software structure is monolithic for all processors. The main processor AT91SO51 software has three software modules:

- The ROM, which verifies the integrity of the Boot loader
- The Boot Loader, in charge of loading and verifying the application
- The application, supporting the TOE security functionality.

61. The TOE is described in [ST, Sections 2 and 10].

TOE Design Subsystems

62. The high-level TOE subsystems, and their security features/functionality, are:

Sub-Systems		
Short name	**Description**	**Type**
Firmware Update	Allows download of new firmware into flash, verifies firmware signature and updates.	SFR-enforcing
Integrity Checking	Periodically calls the firmware checking functions to verify integrity of the firmware.	SFR-enforcing
Device Management	Manages device lifecycle and global state, initialisation, de-initialisation	SFR-supporting
ROM Loader	Handles initial start up of device	SFR-supporting
SBOOT	Handles initial start up of device, verifies integrity of firmware at load. Allows reloading of firmware from within the DPS Key Injection Facility, or starting the SCR application.	SFR-enforcing
Display Services	Manages output of messages visible to the card holder	SFR-enforcing
Key and PIN Entry	Manages input of keys from the card holder. Manages PIN entry and output a pin block.	SFR-enforcing
Buzzer	Outputs auditable tones	SFR-enforcing
UART	Manages communication between physical components.	SFR-supporting
StripeApplication	Handles transaction logic for magnetic stripe transactions	SFR-enforcing
ICCApplication	Handles transaction logic for ICC based transactions.	SFR-enforcing
DUKPT	The DUKPT channel provides a secure link between the DPS and the SCR.	SFR-enforcing
SCR-SKP Link	The SCR+SKP channel provides a secure link and pairing between a SCR and SKP.	SFR-enforcing
ICCReader	Establishes communication channel between SCR and Card Holder ICC	SFR-enforcing
MSR	Magnetic Card Reader - responsible for collecting track 1, 2, 3 data, encrypting it and transmission to the security processor.	SFR-enforcing

Data Storage	Provides persistent storage of data	SFR-supporting
Key Storage	Storage of cryptographic keys	SFR-supporting
Message Storage	Storage of untransmitted or processed messages	SFR-supporting
Configuration Storage	Storage of prompt table, CPT, kernel configuration	SFR-supporting
Firmware Update Storage	Storage of firmware images pending installation	SFR-supporting
Key Loader	Allows cryptographic keys to be injected from within the DPS Key Injection Facility.	SFR-enforcing
Cryptographic Services	Provides asymmetric, symmetric and hashing operations for various subsystems.	SFR-enforcing
Grid Monitor	Responsible for tamper detection and response. Monitors for any physical compromise by monitoring physical tamper meshes. This includes the SCR grid, SKP grid and the MSR grid. When compromised, destroys the master key and puts the device into an inoperable state.	SFR-enforcing
Configuration Update	Responsible for downloading new configuration data for various subsystems.	SFR-supporting
Serial Command Processor	Responsible for parsing SCR serial commands and delegating requests to various subsystems	SFR-supporting

TOE Dependencies

63. The TOE has no dependencies.

TOE Security Functionality Interface

64. The external TOE Security Functionality Interface (TSFI) is:

TSFI		
Short name	**Description**	**Type**
	Physical Interfaces	
Keypad	Secure PIN entry	SFR-enforcing
Display	Display to communicate commands to the card holder on how to proceed with a transaction.	SFR-enforcing
MSR	Read magnetic stripe data (Track 1, 2, 3) from a card.	SFR-enforcing
ICC Reader	Physical secured communication to the ICC of a card.	SFR-enforcing
SCR COM 1	Serial channel to a controller unit.	SFR-supporting
Buzzer		SFR-enforcing

	SCR Serial	
CFG FINS	Install new firmware if there is an image to install	SFR-supporting
CFG SETD	Set POS Device ID and minimum protocol version supported by POS	SFR-supporting
CFG SHUT	Shutdown / Sleep Mode	SFR-non-interfering
CFG LUM	Set system levels for display and pin pad illumination	SFR-non-interfering
CFG SETC	Reconfigures com port parameters, baud rate, queue size.	SFR-supporting
DATA REGD	Register callback notification to controller when SCR configuration has changed	SFR-non-interfering
DATA GETD	Retrieve new settings data that REGD signals	SFR-non-interfering
TXN AUTH	Authorise	SFR-supporting
TXN COMP	Complete approved authorisation	SFR-supporting
TXN VOID	Cancel Transaction	SFR-supporting
TXN PUR	Purchase	SFR-supporting
TXN REF	Refund	SFR-supporting
TXN GET1	Get Transaction Information	SFR-supporting
TXN GETR	Get Transaction Receipt Suitable for Printing	SFR-supporting
TXN CINFO	Upload Cash information transaction	SFR-supporting
TXN OEMD	Download OEM data for last transaction	SFR-supporting
MSG TXEN	Enable or Disable Transmit from SCR	SFR-supporting
MSG TX	Transmit Message from SCR to POS	SFR-enforcing
MSG RX	Transmit message from Host to SCR	SFR-enforcing
L1 CDI	Card inserted event	SFR-supporting
L1 CDO	Card removed event	SFR-supporting
L1 CDTK	Card token	SFR-supporting
ATH GETK	Retrieves random key from DPS HOST. This provides isolated key storage for customer use.	SFR-non-interfering
ATH GETT	Retrieves a security token that the SCR stores, which is periodically updated from the host. The client can then use this token to authenticate itself to the DPS host on other interfaces.	SFR-non-interfering
PP ENTD	Display text based on prompt id and read data from SKP keypad.	SFR-enforcing
STS GS1	Request status information, get online and availability status and current time.	SFR-supporting
STS GSX	Request extended status information	SFR-supporting

STS BTN	Used by the POS to send a button press to the SCR. This is used for the Cancel command only to allow a transaction to be canceled by external device.	SFR-supporting
STS LOG	Retrieve a Log Event (Uses circular buffer limited to 10 log events)	SFR-non-interfering
DSP BUZZ	Invoke buzzer	SFR-supporting
DSP DISP	Display Text based on prompt id	SFR-supporting
	HOST	
HOST_MSG_TYPE_CONFIG_2	Download Configuration	SFR-supporting
HOST_MSG_TYPE_APP_UPDATE	Download Firmware Signature	SFR-enforcing
HOST_MSG_TYPE_APP_SIGNATURE	Download Firmware Signature	SFR-enforcing
HOST_MSG_TYPE_REQ_KEY	Download Offline Privacy Key	SFR-non-interfering
HOST_MSG_TYPE_LOGON	Send Logon Request	SFR-enforcing
HOST_MSG_TYPE_STATIONPARAMS	Download Station Parameters	SFR-supporting
HOST_MSG_TYPE_ADVICE	Send Completion Advice	SFR-enforcing
HOST_MSG_TYPE_REVERSAL	Send Reversal Advice	SFR-supporting
HOST_MSG_TYPE_AUTHORISATION	Send Transaction	SFR-enforcing
HOST_MSG_TYPE_OFFLINE_AUTH	Send Transaction	SFR-enforcing
HOST_MSG_TYPE_FINANCIAL	Send Transaction	SFR-enforcing
HOST_MSG_TYPE_OFFLINE_ADVICE	Send Transaction	SFR-enforcing
HOST_MSG_TYPE_OFFLINE_REFUND	Send Transaction	SFR-enforcing
	SCR Injection	
CMD_CODE_SCR_INJECT_ME	SCR requests injection	SFR-supporting
CMD_CODE_SCR_INJ_START	Start SCR key loading	SFR-supporting
CMD_CODE_SCR_INJ_END	End SCR key loading	SFR-supporting
CMD_CODE_SCR_INJ_PED_PKMFG_KEY	Inject PED PKmfg	SFR-enforcing

CMD_CODE_SCR_INJ_PED_PKCR_KEY	Inject PED PKcr	SFR-enforcing
CMD_CODE_SCR_INJ_PED_SKCR_KEY	Inject PED SKcr	SFR-enforcing
CMD_CODE_SCR_INJ_MAGHEAD_KEY	Inject magnetic head Key	SFR-enforcing
CMD_CODE_SCR_HARDWAREINFO	Tell SCR what its hardware config is	SFR-supporting
CMD_CODE_SCR_INJ_FOREIGN_INJ_KEY	Inject foreign inject keys* (Not used for UK terminals)	SFR-non-interfering
CMD_CODE_SCR_INJ_KEY_TRANSPORT_KEY	Inject Key Transport Key	SFR-non-interfering
CMD_CODE_SCR_INJ_DUKPT_KEY	Inject SCR DUKPT key	SFR-enforcing
CMD_CODE_SCR_TLV_CMD	Allows sending of the above commands TLV format.	SFR-supporting
	SCR Injection	
CMD_CODE_PED_INJ_START	SKP request injection	SFR-supporting
CMD_CODE_PED_INJ_KEY_ESKMFG_PKPP	Inject PED PKpp	SFR-enforcing
CMD_CODE_PED_INJ_KEY_PKMFG	Inject PED PKmfg	SFR-enforcing
CMD_CODE_PED_INJ_KEY_SKPP	Inject PED SKpp	SFR-enforcing
CMD_CODE_PED_INJ_END	SKP end injection	SFR-supporting
	SBOOT	SFR-enforcing

V. TOE TESTING

Developer Testing

65. The developer test plan covers the following areas:

- SCR200 Regression Test (75 test cases)
- Remote Firmware Update Tests (15 test cases)
- PIN Support Tests (SKP200) (36 test cases)
- Other Functionality Tests (91 test cases)
- CA Profile Tests (20 test cases)
- CPT Test (24 test cases)
- PXHOST Tests (9 test cases)
- UK Scheme Tests (2 test cases)
- Key Injection Tests (7 test cases)
- Installation / Activation tests (4 test cases)
- Hardware test (18 test cases)

66. The evaluator selected a sample of the developer test cases to be repeated (7 test cases) focusing on those test cases intended to verify the proper reaction of the TOE to abnormal or malicious behaviour of the external interfaces. The supporting tools developed by the vendor have been used, though some test cases required manual modification of the firmware image file, or modification or deletion of the firmware signature file.

67. The developer test cases are mainly focused in verifying the correct behaviour of the TOE under normal operational conditions. The evaluator decided to supplement these tests with a number of test cases (8) intended to verify the correct reaction of the TOE in regard of abnormal or malicious actions taken by the external entities connected to the TOE.

68. The evaluators devised 11 penetration test cases after the Vulnerability Analysis, intended to confirm or reject the existence of actual weaknesses.

69. The following equipment and or hardware were used for the testing activities:

Equipment
UL Transaction Security Lab in-house EM pulse test bench
UL Transaction Security Lab in-house SPA/DPA, SEMA/DEMA bench
UL sound recording bench
Climatic chamber ESPEC MC-811

70. The following software tools were used for the testing activities:

Tool name	Developer	Version
FirmwareLoader.exe	Payment Express	1.012
PXUPTEMUL.exe (POS emulator)	Payment Express	1.0.2.1
PXMI3 (Web interface emulator)	Payment Express	#139
PXHOST (Host simulator)	Payment Express	#395
PXUPLINK (Acquirer emulator)	Payment Express	#2559
PXHSMSIM (HSM emulator)	Payment Express	#2559
Audacity	Open source	v2.0.6
Octave	Open source	v3.6.4
NIST SP800-22 test suite	NIST	STS v 2.1.2
Zeus	UL	V4.1 build 12.12.11
Serial tool	UL	v 03.03

71. The Developer’s security tests covered:

- all SFRs;
- all TOE high-level subsystems, as identified in Chapter IV (in ‘TOE Design Subsystems’) of this report;
- all TOE Security Functionality;
- the TSFI, as identified in Chapter IV (in ‘TOE Security Functionality Interfaces’) of this report;

72. The Developer’s security tests also included those TOE interfaces which are internal to the product and thus had to be exercised indirectly. The Evaluators witnessed/repeated a sample of the Developer’s security tests.

73. The developer has created a complete test environment which includes test cards, and a simulation of the POS controller and the remote servers for transaction processing and TMS, based on a MS Windows platform. The TOE is connected to the testing PC through a USB port (converted to RS-232) and the connection between the POS controller and the remote server is emulated through an internal IP connection.

74. This test environment has also been provided to the evaluators as a virtual machine.

Evaluator Testing

75. The Evaluators devised and ran a total of 8 independent security functional tests, different from those performed by the Developer. No anomalies were found.

76. The Evaluators also devised and ran a total of 11 penetration tests to address potential vulnerabilities considered during the evaluation. No exploitable vulnerabilities or errors were detected.

77. The Evaluators completed their penetration tests on 8 January 2015.

Vulnerability Analysis

78. The Evaluators' vulnerability analysis, which preceded penetration testing and was reported in [ETR], was based on public domain sources and the visibility of the TOE provided by the evaluation deliverables.

VI. REFERENCES

[AG]	Administration Guide, Payment Express Ltd., SCR200 / SKP200 Hardware Installation Guide, Issue 2.1, July 2014.
[DG1]	Developer's Guide Payment Express Ltd. SCR200 Development Kit – Quick Guide for POS Developers, version 0.3.
[DG2]	Developer's Guide Payment Express Ltd. DPS SCR200 Serial Communications – DPS SCR200 Serial Message Specification, version 1.6.48.
[CC]	Common Criteria for Information Technology Security Evaluation (comprising Parts 1, 2, 3: [CC1], [CC2] and [CC3]).
[CC1]	Common Criteria for Information Technology Security Evaluation, Part 1, Introduction and General Model, Common Criteria Maintenance Board, CCMB-2012-09-001, Version 3.1 R4, September 2012.
[CC2]	Common Criteria for Information Technology Security Evaluation, Part 2, Security Functional Components, Common Criteria Maintenance Board, CCMB-2012-09-002, Version 3.1 R4, September 2012.
[CC3]	Common Criteria for Information Technology Security Evaluation, Part 3, Security Assurance Components, Common Criteria Maintenance Board, CCMB-2012-09-003, Version 3.1 R4, September 2012.
[CCRA]	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security, Participants in the Arrangement Group, 2nd July 2014
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Common Criteria Maintenance Board, CCMB-2012-09-004, Version 3.1 R4, September 2012.
[CEM_POI]	Joint Interpretation Library – CEM Refinements for POI Evaluation, v1.0 (for trial use), 27th May 2011
[PP]	Point of Interaction Protection Profile, v2.0, 26th November 2010
[ETR]	Evaluation Technical Report, UL Transaction Security CLEF, LFU/T003/ETR, Issue 1.2, March 2016.

[JIL]	Joint Interpretation Library, (comprising [JIL_AM], [JIL_AP], [JIL_ARC] and [JIL_COMP])
[JIL_AM]	Joint Interpretation Library – Attack Methods for POI. v1.0 (for trial use), 9th June 2011
[JIL_AP]	Joint Interpretation Library – Application of Attack Potential to POIs, v1.0 (for trial use), 09th June 2011
[JIL_ARC]	Security Architecture requirements (ADV_ARC) for smart cards and similar devices, Joint Interpretation Library, Version 2.0, January 2012.
[JIL_COMP]	Composite product evaluation for Smart Cards and similar devices, Joint Interpretation Library, Version 1.2, January 2012.
[MRA]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, Management Committee, Senior Officials Group – Information Systems Security (SOGIS), Version 3.0, 8 January 2010.
[ST]	Security Target, Payment Express Ltd, DPS SKP200 / SCR200 Common Criteria Security Target, Issue 1.0, Feb 2015.
[UKSP00]	Abbreviations and References, UK IT Security Evaluation and Certification Scheme, UKSP 00, Issue 1.8, August 2013.
[UKSP01]	Description of the Scheme, UK IT Security Evaluation and Certification Scheme, UKSP 01, Issue 6.6, August 2014.
[UKSP02P1]	CLEF Requirements - Startup and Operations, UK IT Security Evaluation and Certification Scheme, UKSP 02: Part I, Issue 4.5, August 2013.
[UKSP02P2]	CLEF Requirements - Conduct of an Evaluation, UK IT Security Evaluation and Certification Scheme, UKSP 02: Part II, Issue 3.1, August 2013.

VII. ABBREVIATIONS

This list of abbreviations is specific to the TOE. It therefore excludes: general IT abbreviations (e.g. GUI, HTML); standard CC abbreviations (e.g. TOE, TSF) in CC Part 1 [CC1] and UK Scheme abbreviations and acronyms (e.g. CLEF, CR) in [UKSP00]

HMAC	Hash-Based Message Authentication Code
IC	Integrated Circuit
ICCR	Integrated Circuit Reader
JIL	Joint Interpretation Library
MSR	Magnetic Stripe Reader
OSP	Organisational Security Policy
POI	Point Of Interaction
RSA	Rivest-Shamir-Adleman
SFR	Security Functional Requirement
TDES	Triple-DES, NIST SP800-67

VII. CERTIFICATE

The final two pages of this document contain the Certificate (front and back) for the TOE.

CESG Certified Product

Common Criteria

P293

This is to certify that

Payment Express Limited

SCR200/SKP200, Version

	SCR200	SKP200
Software Version	• DPSSCR200 v1.3.0.8A • GridMonitor_SCR200 v1.037 • MagHead_SCR200 v1.02 • SBOOT v2.6	• DPSSKP200 v1.3.0.1A • GridMonitor_SKP200 v1.040 • SBOOT v2.6
Hardware Version	SCR200 version D	SKP200 version B

has been evaluated under the terms of the

Common Criteria Scheme

and complies with the requirements for

Point of Interaction Protection Profile

Version 2.0, 26th November 2010

AUTHORISED BY
DIRECTOR GENERAL
FOR GOVERNMENT
AND INDUSTRY CYBER SECURITY

THIS PRODUCT WAS EVALUATED BY
UL - Transaction Security

DATE AWARDED
13 September 2016

Evaluation is not a guarantee of freedom from security vulnerabilities. This certificate reflects the view of CESG at the time of evaluation. It is the responsibility of users (both prospective and existing) to check whether any security vulnerabilities have been discovered since the date shown on this certificate.

The CESG Certification Body of the UK IT Security Evaluation and Certification Scheme is accredited by the United Kingdom Accreditation Service (UKAS) to ISO/IEC17065:2012 to provide product conformity certification as follows:
Category: Type Testing Product Certification of IT Products and Systems.
Standards: Common Criteria for Information Technology Security Evaluation (CC) EAL1 - EAL7.
Details are provided on the UKAS Website (www.ukas.org).

Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA)

The IT Product identified in this certificate has been evaluated at an accredited and licensed/approved Evaluation Facility or at an Evaluation Facility established under the laws, statutory instruments, or other official administrative procedures of the United Kingdom using the Common Methodology for IT Security Evaluation, version 3.1 and CC Supporting Documents as listed in the Certification/Validation Report for conformance to the Common Criteria for IT Security Evaluation, version 3.1. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification/Validation Report. The Evaluation has been conducted in accordance with the provisions of the Common Criteria Scheme 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 CESG or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by CESG or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

All judgements contained in this certificate, and in the associated Certification Report, are covered by the Arrangement up to EAL 2 only, i.e. the augmentation ALC_DVS.2 and AVA_POI extensions are not covered by the Arrangement.

Senior Officials Group – Information Systems Security (SOGIS)
Mutual Recognition Agreement of Information Technology Security Evaluation Certificates (SOGIS MRA), Version 3.0

The CESG Certification Body is a Participant to the above Agreement. The current Participants to the above Agreement are detailed on the SOGIS Portal (www.sogisportal.eu). The mark (left) confirms that this conformant certificate has been authorised by a Participant to the above Agreement and it is the Participant's statement that this certificate has been issued in accordance with the terms of the above Agreement. The judgements contained in this certificate and in the associated Certification Report are those of the compliant Certification Body which issues them and of the Evaluation Facility which performed the evaluation. Use of the mark does not imply acceptance by other Participants of liability in respect of those judgements or for loss sustained as a result of reliance upon those judgements by a third party.
All judgements contained in this certificate, and in the associated Certification Report, are covered by the agreement.

In conformance with the requirements of *ISO/IEC17065:2012*, the CCRA and the SOGIS MRA, the CESG Certification Body's website (www.cesg.gov.uk) provides additional information as follows:

- Type of product (i.e. product category); and
- Details of product manufacturer (i.e. as appropriate: vendor/developer name, postal address, website, point of contact, telephone number, fax number, email address).

All IT product names and company names used in this certificate are for identification purposes only and may not be trademarks of their respective owners.

Evaluation is not a guarantee of freedom from security vulnerabilities. This certificate reflects the view of CESG at the time of evaluation. It is the responsibility of users (both prospective and existing) to check whether any security vulnerabilities have been discovered since the date shown on this certificate.