SPoC Solution Security Evaluation Criteria

The IAC Code Set, Vol 4: Device Requirements And Cryptographic Management, clause 2.9.2 SPoC Solution Security Evaluation Criteria, sets out the criteria under which a SPoC Solution can be approved for use within Australia.

2.9.2 SPoC Solution Security Evaluation Criteria

This part sets out the minimum security standards for SPoC solutions and the SPoC solution evaluation process.

(a) All SPoC solutions must have been approved by PCISSC and must be listed on the PCISSC website for Approved SPoC Solutions.

(b) The SCRP component of a SPoC solution must meet the relevant PCI Plus security requirements of Annexure B of this Volume.

(c) The Company will assess individually the PCISSC SPoC FAQs for suitability to the Australian payments industry. All SPoC solutions must be evaluated by reference to those PCI SSC SPoC FAQs suitable to the Australian payments industry and listed on the AusPayNet Approved SPoC Solutions website. The Company will formally communicate each unacceptable FAQ to the SPoC Solution Approved Evaluation Facilities.
(IAC version 8 – effective 1 January 2019)

Acceptability of Magnetic Stripe Readers in SPoC Solutions in Australian Payments Network.
As per Clause 2.9.2 (c) above AusPayNet evaluates the acceptability of each individual PCI-SSC SPoC FAQs [2] for acceptability for use within the Australian payments industry. The evaluation and approval of all SPoC solutions [4] by AusPayNet must be made with reference the PCI SSC SPoC FAQs [2] acceptable to the Australian payments industry as listed here.

AusPayNet has formally communicated to the SPoC Solution Approved Evaluation Facilities. which PCI SP0C FAQs are unsuitable for use within Australia: see Table below.

The use of magnetic strip readers and EMV magstripe mode
As of May 2019, AusPayNet reviewed FAQ 8 and 9 [2] and deemed them unacceptable for the Australian market. Consequently, the Magstripe Reader Annex [1] is not acceptable for the use of a SPoC solution [3][4] with either EMV magstripe mode or a magstripe reader within Australia.

Software-based PIN Entry on COTS™ Technical FAQs Technical FAQs, May 2019,

PCI Security Standards Council.

General Questions		Suitability for the Australian payments Industry
Q1	**Are contactless transactions allowed under the SPoC Standard?**	**Yes**
A	*Yes. The Standard supports both EMV-based and magnetic stripe mode contactless transactions.* *[AusPayNet Comment: Please be aware that "magnetic stripe mode contactless transactions" are still contactless chip based transactions.]*	
Q2	**In the SPOC TRs, where the attack costing thresholds are required, there is no minimum to be met. When will the attack costing threshold values be added and how should labs evaluate the relative requirements in the interim?**	**Maintain Watching brief as attack costings are developed**
A	*The PCI SSC will be working directly with the labs that are qualified to perform Solution assessments. Each assessment will be used to contribute relative attack costing information using actual Solution validation data that will factor in to the development of appropriate attack costing values. Once sufficient data has been obtained a revision to the Test Requirements will be published with the inclusion of these values.*	
Q3	**Please explain the difference between a "session" and a "transaction" within the context of the Software-based PIN Entry on COTS (SPoC) standard?**	**Informational**
A	*A "session" is established when the PIN CVM Application is used to initiate a payment. This session includes establishing secure channels with the SCRP and with the back-end monitoring system. The session is terminated once the payment has completed or if any anomalous behaviour is detected in The Solution at any point during the payment process.* *A "transaction" consists of the payment processing messages created and sent to and from the back-end payment processing systems to gain authorization for a customer.*	
Q4	**Regarding "Customer Data" and "Correlatable Data", what is the scope of this data?**	**Yes**
A	*The scope applies to data that is entered into a PIN CVM Application on a COTS Device as part of the payment transaction process or sent from the Back-end Monitoring System to the COTS Device. The scope is limited to data entered by the cardholder at the time of the transaction for purposes such as receipt transmission.*	
Q5	**What are the use cases for a SPoC Solution?**	**Yes**
A	*SPoC Solutions are intended to be used in a face-to-face environment where the merchant hands the COTS device to the customer. The customer then enters their PIN and hands the COTS device back to the merchant.* *SPoC Solutions are not intended for environments where the device is part of a kiosk (semi-attended or self-checkout) or Automated Fuel Dispenser. These are unattended environments and pose a*	

	greater risk of compromise and are not permitted under this standard.	
Q6	**What is the intent of use of a SPoC Solution in an attended versus an unattended environment?**	**Yes**
A	*The intent of the SPoC standard is for merchant COTS devices in attended environments. Attended environments are when the COTS device is made available to the customer by the merchant during a payment transaction. For example, the merchant handing the COTS device to the customer. The customer enters their PIN and hands the COTS device back to the merchant.* *Merchant COTS devices in unattended environments pose a higher risk of compromise and are not permitted under this standard. Unattended environments would mean the COTS device is not handed to the customer by the merchant or merchant staff but rather the COTS device is part of a kiosk (semi-attended or self-checkout) or of a vending machine with no merchant involvement at the time of the transaction.*	
Q7	**Is Software-based PIN Entry on COTS (SPoC) synonymous with PIN on Glass?**	**Information**
A	*No. The SPoC Standard covers a software-based approach to for accepting PIN as the cardholder verification method on a merchant owned COTS device. The phrase "PIN on Glass" is often used generically regarding a variety of use cases, with the commonality simply being entering a PIN value on to a glass-based capture mechanism (i.e., a touch screen) on a variety of device types.* *A SPoC Solution includes an SCRP (Secure Card Reader – PIN), a PIN CVM application, the merchant's COTS device as well as back-end monitoring and attestation systems. These elements all work together to ensure the PIN, accepted by a software application on the COTS device, is isolated within the COTS device from other sensitive account data. The back-end monitoring and attestation systems continuously monitor the entire solution for anomalous activity and to ensure The Solution has not deviated from the baseline (i.e. tampering, rooting or physical attacks). In other words, within a SPoC Solution, the merchant-facing COTS device is only one element of the entire Solution, whereas a POI device is generally a single device.* *There are numerous PCI PTS approved hardware-based point of interaction (POI) devices for acceptance of PIN using a touch screen (i.e., "PIN on Glass"). These POI devices are purposely built for payment acceptance. Therefore, care must be taken when using the generic phrase "PIN on Glass", as, for example, a PTS-approved POI device that accepts PIN on Glass is very different from a SPoC Solution that uses a merchant-facing COTS device to accept PIN.*	
Q8	**Are magnetic stripe-based transactions allowed by the Software-based PIN Entry on COTS Standard?**	**No:** For purposes of clarity be aware that transactions originating from magnetic stripe data are **NOT** accepted via SPoC Solutions in Australian**.**
A	*Yes. The Standard supports both EMV-based and magnetic-stripe mode-based contactless transactions. It also optionally supports the contact magnetic stripe reads. Contact magnetic stripe reads must only occur using a separate Magnetic Stripe Reader (MSR) Device that complies with the SPoC Annex, and the PIN CVM Application must prevent the entry of the PIN.*	

Q9	**Can a merchant use their existing SCR to accept payments in a SPoC Solution?**	**No:** Any SPoC Solution which includes magnetic stripe functionality is prohibited from implementing that functionality in Australia and any SCRP which include magnetic strip readers will **NOT** be approved.
A	*Merchants can use PCI-approved SCRPs for chip-based transactions. Contact magnetic stripe reads must only occur using a separate MSR Device that complies with the SPoC Annex, which might include existing approved PCI PTS SCRs.*	
Q10	**Can a merchant put together their own SPoC solution by choosing a SCRP, PIN CVM Application and back-end monitoring system?**	**Yes**
A	*No. Only complete SPoC Solutions will be approved and listed on the PCI SSC website.*	
Q11	**What constitutes a SPoC Solution? Does the SPOC standard cover separate components or is it a single solution?**	**Yes**
A	*A The SCRP will have a separate listing because it is evaluated and listed as part of the PTS POI Standard. However, all SCRPs associated with a SPoC Solution will be included as part of the SPoC Solution evaluation and listed as part of that SPoC Solution's acceptance. It is also possible that an MSR evaluated as part of SPoC Solution might have a separate listing if it is evaluated and approved as a Secure Card Reader (SCR) as part of the PTS POI Standard.* *A SPoC Solution consists of PCI-approved SCRPs, an optional MSR that complies with the SPoC Annex, a PIN CVM Application, merchant COTS Devices, and Back-end Monitoring/Attestation Systems. The SPoC Solution will be listed on the PCI SSC Website with the individual elements.*	
Q12	**What is a COTS device?**	**Yes**
A	*A commercial-off-the-shelf (COTS) device is a mobile device (i.e. smartphone, tablet or wearable) that is designed for mass-market distribution and is not designed specifically for payment processing.*	
Q13	**Is a Software-based PIN Entry on COTS Solution eligible for a P2PE Solution approval?**	**Yes**
A	*No. The Software-based PIN Entry on COTS (SPoC) Standard and the P2PE Standard are separate PCI SSC standards intended for unique use cases.*	
Q14	**Are there any restrictions to the specific form factors for COTS devices and SCRPs which can be approved under the PCI SPoC program?**	**Yes**
A	*No, the SPoC requirements do not dictate any specific form factor for the COTS device, the SCRP or the combination thereof for inclusion in an approved and validated SPoC Solution.*	
	SPoC Security Requirement 2.2	
Q15	**Is it possible to include an operating system (OS) version in the COTS System Baseline of the initial Solution evaluation that is not supported by the OS vendor at the time of evaluation?**	**Yes**
A	*No, Security Requirement 2.2.2 requires that PIN CVM Applications must be developed only for operating systems that are still supported by the operating system vendor. All new Solutions must operate only on supported platforms. The initial COTS System Baseline must not include any version of a COTS OS that is not*	

	supported by the OS vendor at the time of the initial evaluation.	
Q16	**Security Requirement 2.2.3 states that the PIN CVM Application must only support platforms that provide for a “trusted boot” mechanism that validates the operating systems authenticity. What are the implications of this requirement recognizing that for certain Android versions (such as Android 4), some OEMs did not support sufficient hardware capabilities to implement the secure boot mechanism? What are the implications associated with scenarios where a clear designation of trust boot support of “yes or no” cannot be determined?**	**Yes**
A	*For scenarios where such Android versions and OEM implementation are supported in the COTS System Baseline, the Lab must detail these conditions and any additional controls that are in place to mitigate the risks. Furthermore, the SPoC Lab must demonstrate that such supported COTS systems do not represent a significant portion of the supported customer base.*	
Q17	**Does Security Requirement 2.2.3 include OS level or other system applications?**	**Yes**
A	*No. This requirement is not intended for OS level or other system applications.*	
Q18	**Security Requirement 2.2.5 states that where white-box cryptography is used, white-box keys must be unique for each PIN CVM Application instance, and that the reliance upon and use of common white-box keys must be minimized after the secure provisioning process. Does this requirement apply to all white-box keys as it relates to unique keys per PIN CVM Application, or just those used for encrypting a PIN?**	**Yes**
A	*The intent of the requirement is that where white-box cryptography is used, each PIN CVM Application instance must use unique keys for PIN encryption. White-box keys shall be updated when the PIN CVM Application is updated, which is at least monthly in accordance with Security Requirement 2.5.6.*	
	SPoC Security Requirement 2.4	
Q19	**Security Requirement 2.2.4 states that PIN CVM Application must detect sensor activation and polling of sensor data. Does this requirement apply to all COTS Platforms?**	**Yes**
A	*The intent of the requirement is to protect PIN entry process from manipulation or subversion. Since several attack vectors use COTS Platform sensors and hardware for side-channel attacks, detecting when these sensors are activated or used (i.e., polling sensor data) by other, untrusted, applications can reduce the risk of PIN compromise. In cases when the COTS Platform does not allow runtime application to detect the status of sensors or sensor data pooling, the Solution Provider should document and substantiate the COTS Platform limitations, and justify how these limitations do not impact the security of PIN entry process.*	
	SPoC Security Requirement 3.2	
Q20	**Security Requirement 3.2.13 states that for manual updates to the attestation system, any deployment changes to the production environment must require dual control. Is dual control necessary for attestation system components associated with the**	

	PIN CVM Application recognizing such applications are signed by the OS App Store and not under the control of the Solution Provider?	**Informational**
A	*It is acknowledged the signing of a PIN CVM Application made available from the OS App Store(s) is not under the control of a PIN CVM Application provider or overall Solution Provider and dual control cannot be enforced for such PIN CVM Applications by a Solution Provider.*	
	SPoC Security Requirement 3.6	
Q21	**SPoC Security Requirements 3.6.1 and 5.1.2 state that if the Back-End Monitoring system resides in the Cardholder Data Environment, then PCI DSS and Appendix A3: Designated Entities Supplemental Validation (DESV) will apply. Does a SPoC Solution Provider have to be fully compliant with DESV when submitting a SPoC Solution for initial validation?**	**Yes**
A	*If the Solution Provider cannot meet DESV requirements at the point of an initial SPoC solution validation, the Solution Provider must provide, to the SPoC lab, an action plan demonstrating that work is in progress for requirements to be met at the first annual checkpoint. The action plan will be reviewed for sufficiency.*	
	SPoC Security Requirement 4.3	
Q22	**If a version of the COTS OS initially listed in the Solution System Baseline reaches end of life such that it is no longer supported by the original OS vendor, is it the intent of the SPOC standard to disallow transactions on affected COTS devices until the OS on those devices is updated to a supported OS?**	**Yes**
A	*No. If a particular OS version has been assessed and is listed as included in the COTS System Baseline, (TR C1) and then that particular instance becomes no longer supported by the OS vendor, then as per Security Requirement 4.3.7 and TR C4, the Solution provider must provide justifications why the acceptance and use of such a platform for accepting PIN entry does not increase the risk of PIN exposure, or subversion of the payment process, beyond use of devices which are supported by security patches as a part of the annual update of the risk-assessment policy and procedure. If such justifications are accepted at time of the review by PCI Council after review of the laboratory evaluation report then the unsupported platform may continue to be used. Such justifications will need to be "re-justified" during each annual Solution evaluation cycle subsequent to any initial Solution approval.* *If such justifications are not provided or are not accepted by the PCI Council, the SPoC standard requires that merchants using the PIN CVM Application on affected platforms be notified by the Solution Provider and that the merchants are migrated to supported platforms. (SR 4.3.7).*	
Q23	**If a new updated version of a COTS OS initially listed in the Solution System Baseline is made available by the original OS vendor, is it the intent of the SPOC standard to disallow transactions on affected COTS devices until the OS on those devices is evaluated?**	
A	*No. If a new updated version of an OS which is already listed in the COTS System Baseline is made available by the original OS vendor*	

	then the Solution Provider may add that version to the COTS System Baseline and must provide justifications for the acceptance and use of such a platform as a part of the annual update of the risk-assessment policy and procedure. If such justifications are accepted at time of the review by PCI Council after review of the laboratory evaluation report then the new platform may continue to be used. *If such justifications are not provided or are not accepted by the PCI Council, the SPoC standard requires that merchants using the PIN CVM Application on affected platforms be notified by the Solution Provider and that the merchants are migrated to supported platforms. (SR 4.3.7).*	**Yes**
SPoC Security Requirement 5.1		
Q24	**SPoC Security Requirements 3.6.1 and 5.1.2 state that if the Back-End Monitoring system resides in the Cardholder Data Environment, then PCI DSS and Appendix A3: Designated Entities Supplemental Validation (DESV) will apply. Does a SPoC Solution Provider have to be fully compliant with DESV when submitting a SPoC Solution for initial validation?**	**Yes**
A	*If the Solution Provider cannot meet DESV requirements at the point of an initial SPoC solution validation, the Solution Provider must provide, to the SPoC lab, an action plan demonstrating that work is in progress for requirements to be met at the first annual checkpoint. The action plan will be reviewed for sufficiency.*	
Q25	***Test Requirement TB2.5 talks about disabling of on-device sensors during PIN entry. Does this requirement apply to all COTS Platform***?	**Yes**
A	*SPoC Standard does not mandate disabling on-device sensors during PIN entry. This requirement only applies if the Solution Provider implemented manual (e.g., via end-user prompt to disable a sensor) or programmatic disabling of on-device sensors.*	

[1] Software-based PIN Entry on COTS™ Magnetic Stripe Readers Annex, May 2019 PCI Security Standards Council.

[2] Software-based PIN Entry on COTS™ Technical FAQs Technical FAQs, May 2019, PCI Security Standards Council.

[3] Payment Card Industry Software-based PIN Entry on COTS Test Requirements, Jan 2018, PCI Security Standards Council.

[4] PCI Software-Based PIN Entry on COTS Security Requirements, v1.0, Jan 2018, PCI Security Standards Council.