Rules

Betaalvereniging Nederland

Procedure for the Security Certification of POI devices

Version 2.01 | 7 April 2015 | proc.cert.POI devices

Betaalvereniging Nederland

Contents

Version history

Version number	Version date	Status	Edited by	Most significant changes
1.0	*11/04/2012*	*final*	*Payments Association*	
1.1	*11/07/2012*	*final*	*Payments Association*	*Add rules for PCI-only POI devices; version numbers of documents removed (refer to most recent version)*
1.2	*11/10/2012*	*final*	*Payments Association*	*Add procedure for non-PIN terminals (separate attachment)*
1.3	*14/03/2013*	*final*	*Payments Association*	*Explanation of periodic reassessment (section 3.4 and 3.5)*
2.0	*25/02/2015*	*Draft*	*Payments Association*	*Reassessment* *Mandatory support of SRED for new certifications from 01/01/2016;* *Procedure for integration of payment terminal in vending machine added;* *Inform acquirer on organisation of payment chain from POI to the acquirer processor.*
2.01	*7/04/2015*	*final*	*Payments Association*	*Review comments processed.*

Disclaimer:

This document is a translation of the Dutch original and is provided as a courtesy only. In the event of any inconsistencies or differences of interpretation between the original and translated versions the Dutch version shall prevail. No rights may be derived from the translated document.

1. General

This Procedure for the Security Certification of POI devices sets out the conditions that suppliers and/or manufacturers of POI devices must fulfil in order to qualify for an approval certificate. The approval certificate is issued by the Dutch Payments Association (hereafter referred to as the Payments Association) and is required for POI devices installed in the Netherlands for which the acquirers are members of the Payments Association (http://www.betaalvereniging.nl/en/members/).

A supplier is a company (suppliers and/or manufacturers of POI devices) that supplies POI devices for connection to the payment infrastructure for electronic payments in the Netherlands, in conformity with the requirements of the Payments Association.

1.1 Certification entity

The Payments Association will perform its certification activities in its role of certification authority. In line with European developments, the work will include the following tasks for POI devices in the market in the Netherlands:

1. Maintaining the certification procedure for POI devices;
2. Issuing approval certificates / security certificates for POI devices, for connection to the payment infrastructure for electronic payments, after successful completion of the certification procedure;
3. Publishing a list of approved POI devices on the designated website;
4. Identifying the underlying payment chain. Underlying payment chain refers to the infrastructure from the certified POI device to the processing systems of the acquiring host processor.
5. Performing risk management in relation to approved operational POI devices and the underlying payment scheme, including:
   - Managing the life cycle of permits issued (expiry of permits based on previously issued security certificates);
   - Monitoring (and following up) incidents in the field (including for fraud management);
   - Reporting any risks in the payment chain to the acquirers responsible.
6. Following up European developments in relation to certification and looking after the members' related interests.

1.2 Scope

The scope of the certification procedure is restricted to security certification of POI devices and integration of unattended POI devices in vending machines. The procedure is rooted in the old PCI+ certification procedure for Dutch domestic brand ‘PIN’, but takes into account European requirements for certification processes as described in Book 4 of the EPC Volume. For illustrative purposes, all of the certifications which a Dutch POI device passes through, including this certification process, are set out in Annex 1 Test and Certification Model for POI devices.

1.3 Certification of non-PED POI devices

The procedure 'Security Certification POS' as outlined above relates to terminals where for making a payment transaction a PIN is entered. Market developments have ensured that POI devices will be available without support of PIN entry (for example, Dip & Go POI devices in the parking sector). Certification is also required for these POI devices. However, because these POI devices have a different (security) risk profile, a different certification process will be used for these non-PED devices. This certification procedure is described in Annex 7.

1.4 Assessment of Privacy Shield

With the exception of POI devices that satisfy the criteria for a handheld device in accordance with the PCI standard, all POI devices for the Dutch market must have a privacy shield that satisfies “EPC343-08 PRIVACY SHIELDING FOR PIN ENTRY” Version 1.4 of 30 September 2009. For unattended POI devices it is acceptable for the privacy shield requirements to be satisfied at the time of integration of the POI device in the vending machine. This procedure is described in Annex 8.

1.5 Structure of the document

Chapter 1 provides a general explanation, describes the parties involved and explains the POI devices to which this certification procedure applies as well as the scope of the certification programme.

Chapter 2 provides an overview of the certification procedure including a reference to the applicable requirements.

Chapter 3 describes the steps in the procedure that will apply specifically to the Dutch market.

2. Overview of criteria to obtain an approval certificate

The approval certificates issued by the Payments Association for security certification of POI devices are based on the European requirements as published by the EPC in Book 4 of the SCS Volume v7.0. The European requirements are based on the physical and logical PCI requirements from the PCI PTS standard, supplemented with EPC PLUS requirements for secure processing of the payment transaction and requirements for the production process of the POI device. A more detailed description of these European requirements (based on the underlying version of the PCI standard) can be found in Annex 2.

From 01/01/2016, there will be an additional requirement that POI devices presented for initial certification must use Secure Reading and Exchange of Data (SRED). The SRED module used must be certified by PCI SSC in combination with the key management scheme used for the Dutch market. A transitional period of 12 months applies to delta certifications. This does not apply to the POI devices for which SRED is not available, such as PCI PED 1.3 and 2.* certified POI devices.

Suppliers must provide the Payments Association with a PCI certificate and the underlying evaluation report, to prove that the PCI requirements have been met. Access to the evaluation report is essential for risk management, one of the tasks associated with the role of a certification entity.

Suppliers must provide the evaluation reports to prove that they have fulfilled the EPC PLUS requirements. These evaluation reports must chronicle the investigation of the EPC PLUS requirements and must only be produced by evaluation labs that have received relevant accreditation from the Payments Association. Next, the evaluation reports are assessed by the Payments Association for accuracy and completeness in order to qualify for an approval certificate.

The PCI certificate and certification of the POI device in accordance with the EPC PLUS requirements by the Payments Association leads to an approval certificate. Suppliers will receive an approval certificate by letter, signed by the board of directors of the Payments Association.

3. Process

A requirement for the certification of POI devices is the presence of a signed Standard agreement for POI device suppliers setting out the agreements between the Payments Association and the supplier.

The Payments Association is the contact point for suppliers to get their POI devices certified. The certification consists of the following phases:

1. The Supplier performs the registration of the terminal with the Payments Association (providing information on the supplier and POI device).
2. Establishment of the payment chain, from the POI device to the transaction-processing systems of the acquirer processor, if applicable. The aim is to obtain insight into which relevant standards are met by the various components as well as how the various components exchange data with one another.
3. The Payments Association performs an evaluation of the research reports provided by the supplier.
4. The Payments Association issues an approval certificate. Approved POI devices are published on the website of the Payments Association.

3.1 Registration of POI device and payment chain

The Payments Association is the contact point for suppliers to get their POI devices certified. The Payments Association will also help to coordinate the subsidiary investigations in the context of the certification. Not only new POI devices need to be registered, but also POI devices that have undergone modifications that may affect security aspects of the POI device (see Annex 2). The objective of the application procedure is to register POI devices submitted for certification and to exchange all the necessary information and requirements for the certification to be completed.

The supplier must also provide insight into the underlying payment chain. This can be done by completing the Certificate of Conformity as described in Annex 6.

3.2 Scope of the Investigation

After consulting the supplier, the Payments Association will determine the scope, on which basis an evaluation lab can perform its investigation. The supplier can choose one of the evaluation labs listed in Annex 10.

Any new type of POI device is subjected to full certification. In the event of modifications to existing types of POI devices, only the impact is assessed and only part of the certification procedure is required. Specifically for modifications to the security software, a distinction is made between high-impact modifications and smaller modifications.

Modifications concerning the security software of the POI device with a potentially large impact must first be submitted to the Payments Association for assessment. Such changes can only be implemented after they have been approved. After all, a risk analysis is required to assess the extent of the potential impact. The analysis will in any case examine all functions responsible for processing the PIN and/or associated key management. Changes in PIN handling and key management are always considered as changes with large impact.

The procedure for small modifications is different. In that case, suppliers are authorised to implement minor changes in the security software of the POI device. This is subject to the condition that the Payments Association is informed of these changes by means of so-called Release Notes with associated risk analysis before the software is put into use in an operational environment. The Payments Association must assess based on the Release Notes whether it indeed concerns a small modification. If necessary, the Payments Association can contact the supplier about it. Small modifications subsequently undergo substantive tests by the Payments Association itself. This test is in any case held within one year from the modification being reported. The test may take the form of a separate action but can also be combined with a major modification of the security software.

An exception is made if it can be demonstrated that the software satisfies PCI PTS 4.* and SRED – or more recent – in which case informing the Payments Association of the implemented changes will suffice. Demonstrated means that the Payments Association has determined at the time of initial certification that the POI device satisfies the EPC PLUS requirements, PCI PTS 4.* and or more recent, and that the SRED module is part of the evaluation for which PCI issued the certificate. In addition, the SRED module must be used for the payment chain about which the Payments Association has been informed.

The supplier must issue a certificate of conformity for each version of the security software (regardless of whether large of small modifications were made) (see Annex 5) in which it states that it only uses security software that has been certified in the event of large modifications, possibly supplemented with small changes as indicated in the form of Release Notes.

The supplier will also have to issue a certificate of conformity (see Annex 6) for each relevant modification in the payment chain, stating that it will use only this payment chain for the members of the Payments Association.

The manner in which this investigation will take place is in accordance with the standards set out in Annex 2.

3.3 Assessment

The research reports produced by the evaluation lab will be made available to the Payments Association. The same applies to the evaluation reports and other certificates showing that the

elements in the payment chain comply with the relevant standards. The Payments Association will evaluate the reports and check them against the requirements set out in Chapter 2

If it finds itself in agreement (with the evaluation report) the Payments Association will inform the supplier in writing. The approval certificate is issued on condition that the supplier issues a certificate of conformity. With this certificate, the supplier undertakes that the POI device will only be commissioned in the operational environment with the security-relevant components that were assessed. The certificate of conformity must cover both hardware and software aspects of the POI device and the underlying payment chain (see Annex 4, Annex 5 and Annex 6).

The certificate of conformity described in Annex 5 for the software must contain a reference to the method specified by the Payments Association to guarantee the authenticity of the software. Other methods of at least equal value will be considered through consultation.
In addition, the supplier will be given the opportunity to perform a Build&Sign procedure with the Payments Association. The advantage of this procedure is that the supplier is protected against later disputes concerning software in use in the field. Only software authorised by the Payments Association may be used in the field.

In the event the Payments Association decides to refuse (based on the evaluation report) it will inform the supplier of its decision in writing, stating its reasons. Suppliers wishing to appeal a refusal can submit their dispute to the NAI pursuant to Article 8 clause 2 of the Agreement for POI device suppliers.

In the event of a refusal, suppliers have the option of resubmitting the POI device to the Payments Association after modifying the POI device or adjusting the evaluation report.

In specific circumstances, the Payments Association may grant dispensation under certain conditions despite the evaluation report not being fully ratified. The Security Working Group will be consulted in relation to any dispensation that may have a relevant impact for acquirers. The Payments Association retains the final decision on granting any dispensation.

3.4 Permitted sales and use period of the POI device

The sales period is determined by the validity term of the underlying PCI certificate. As yet, no rules have been agreed for the sales period for SEPA. The PCI SSC regulations are used as a starting point for this certification procedure, which means a potentially long sales period of 10 years. In order to minimise the associated risks, the Payments Association imposes an additional requirement. The requirement entails that the security certificate must be kept up to date. This means that the Payments Association reserves the right to conduct a reassessment, for example in response to new technological developments. The reassessment consists of the Payments Association re-evaluating the POI device in respect of the latest developments and attack techniques (by means of desk research) based on available evaluation reports (initial reports and any delta reports). On that basis the Payments Association, in consultation with the supplier, determines whether there is any need for a further investigation.

If further investigation shows that a POI device no longer satisfies the standards, the Payments Association will evaluate the impact of the deviation and any consequences for the security certificate (such as an earlier expiry date) in consultation with the terminal supplier. Other risk mitigation measures are also possible. These measures shall be determined in consultation with the supplier.

The period of use of the POI device (after the expiry date of the security certificate) is determined by regulations from the card schemes. In the absence of such regulations, POI devices may be used in an operational environment for a maximum of five years after the security certificate expires, which is the so-called 'five-year sunset rule'). In exceptional circumstances, when serious security problems arise, this period may be cut short for a certain type of POI device. If necessary, the Payments Association may contact the market parties concerned.

Further details on the PCI SSC rules in accordance with the underlying PCI standard in combination with the additional measure of periodic reassessment can be found in Annex 3.

3.5 Costs and turnaround times

The total turnaround time of the certification procedure by the Payments Association strongly depends on the availability and quality of the submitted reports. On average, the turnaround time between the Payments Association receiving all the necessary reports and giving a definite answer on whether the request is approved or refused is two weeks.

The costs for all investigations concerning the POI device by the evaluation labs accredited by the Payments Association shall be borne by the supplier. The Payments Association will not charge the supplier for issuing the approval certificate and the publication thereof on the Payments Association's website.

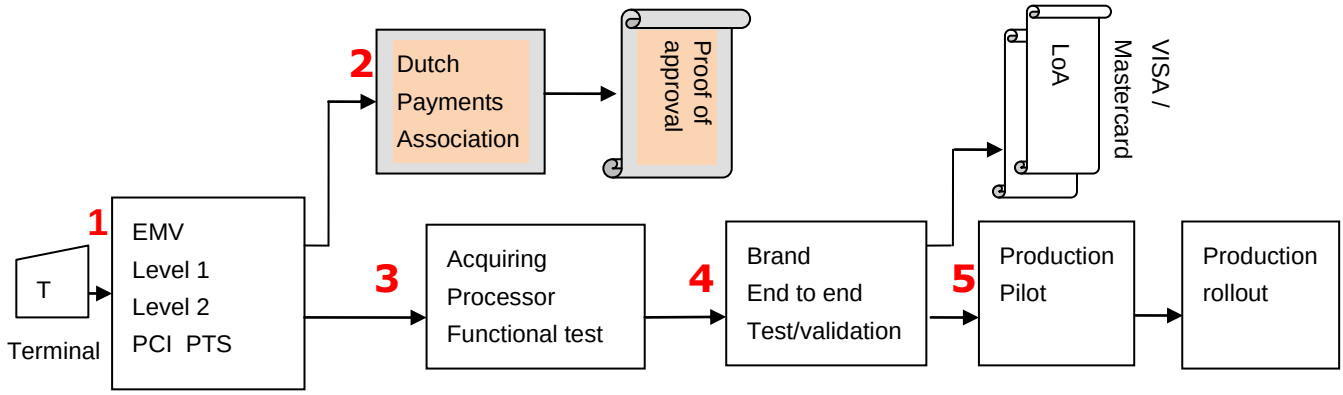
The costs for reassessment for maintenance of the certificate shall be borne by the Payments Association.

The costs for the first two assessments of the integrated privacy shield shall be borne by the Payments Association, with the exception of any travel and accommodation expenses incurred by the Payments Association for the assessment. If the instructions of the Payments Association are not followed, the Payments Association will charge for the costs incurred for a third assessment, at a basic rate of EUR 1,250 excluding VAT per working day.

Annex 1. Test and Certification Model for POI devices (INFORMATIVE)

This appendix paints the overall picture of certification and admission for a Dutch POI device and the place of the Payments Association's security certificate within this picture.

Schematic presentation:



Key:
2. Dutch Payment Association → Proof of approval
3. Acquiring Processor Functional testing
4. MC/VISA End test/Validation → VISA/Mastercard Certificate
5. Production Pilot Production Rollout

The Procedure for the Security Certification of POI devices referred to in the document below exclusively relates to the aforementioned Step 2.

Step 1
This step includes the certifications prescribed by the global schemes:

- EMV level 1, for the hardware certification of the chip card reader
- EMV level 2, the software for processing the chip card on the POI device
- PCI PTS, covers, among other things, the security requirements in relation to the POI device

Step 2

This step checks for the presence of the above-mentioned certificates or approvals. These certificates must be available for submission to the Payments Association.

The security certification of Dutch POI devices is as follows:

a. A further evaluation of the POI device by an accredited evaluation lab (see Annex 10) against the standards as published in the most recent EPC Volume (see Annex 2).
   The evaluation consists of the following components:
   - A hardware investigation (including a check on the Privacy Shield);
   - A software investigation (code review) of the PED firmware;
   - An investigation of the production procedures for the POI device, including the initialisation of the vendor keys;
   - An investigation of security services for the safe processing of the payment transaction by the payment application (e.g. safe communication with the acquiring host)

b. The supplier submits the report of the evaluation lab to the Payments Association.

c. The Payments Association evaluates the report (quality, completeness, findings, appraisals).

d. The Payments Association issues an approval certificate.

It is thought to be more time and cost-effective to arrange evaluations for PCI PED/PTS (see Step 1) and EPC PLUS simultaneously.

Step 3

The Acquiring Processor tests consist of:

a. Functional testing of the POI device by a test lab. (For CTAP these are the FAT tests under the responsibility of Acquiris)

b. Testing of the POI device against the host. (For CTAP these are the NDT tests under the responsibility of the Acquiring Processor)

Step 4

The EMV production tests on the Acquiring Host systems consist of:

a. MasterCard,Terminal Integration Process (TIP)
b. VISA, Acquirer Device Validation Tool
c. Where applicable: End-to-End tests including LBs (such as 13.005_LB_bindend_Regelgeving-Uitbreiding-Brand-testen-v1-0)

With MasterCard and VISA (global schemes) these additional end tests lead to a certificate authorising connection of the POI device to the host system of the Acquiring Processor concerned.

Step 5

This step concerns the overall testing of the POI device:

a. For its correct operation on the Acquiring production Host (pilot)
b. In relation to any other Acquiring Processor products/services

A limited number of POI devices are rigorously monitored under the responsibility of the Acquiring Processor, to examine how these POI devices function while in production. After successful completion of the tests, the Acquiring Processor can decide to grant the supplier permission to link up the POI device for production.

A prerequisite for this procedure is that the certificates or approvals obtained in Step 1 are ready and available. The certificates or approvals must be submitted to the Payments Association.

Annex 2. Applicable requirements

Operational POI devices in the Dutch market are subject to the European requirements as published by the EPC in its Book 4 of the SCS Volume. .
The most recent version (7.0) of this document can be found at:
http://www.europeanpaymentscouncil.eu/index.cfm/sepa-vision-for-cards/sepa-cards-standardisation-volume-version-70-published-in-2014-ready-for-market-implementation/

The European requirements are in addition to the requirements of the global schemes. These requirements have been drawn up by PCI SSC for the global schemes. The following PCI standards are relevant:

- PCI PED 2.x, A (physical) , B (logical) , C (online PIN) and D (offline PIN) requirements
- PCI PTS 3.x, A, B, C and D requirements (CORE module), E requirements (Integration module). Furthermore, an OP module for protection of data over open, public (Internet and WiFi) connections and an optional SRED module for protection of card holder data (PAN).
- PCI PTS 4.x, see PTS 3.x.

The following EPC PLUS requirements apply to the following PCI standards.

- PCI PED 2.x : privacy shield, code review PED firmware, production procedures, security services for payment application for secure payment transaction.
- PCI PTS 3.x: the same supplementary requirements as for PED 2.x
- PCI PTS 4.x: privacy shield, production procedures, security services for payment application for secure payment transaction.

PTS 4.x eliminates the need for the supplementary requirement of code review PED firmware.
PTS 3.x and PTS 4.x including the OP and SRED modules can also provide the security services for the payment application for a secure payment transaction.

The following publications are important for a further explanation (guidance) of the EPC PLUS requirements and the relationship with underlying PCI requirements.

- EPC343-08 Privacy Shielding for PIN Entry, version 1.4
- EPC PLUS POI DTR, version 2.0 drawn up by the Payments Association [update of CAS POI DTR version 1.1.a, **currently under review**].

PCI guidance is available on the PCI SSC website, see:

- https://www.pcisecuritystandards.org/security_standards/documents.php?association=PTS

EPC PLUS POI DTR guidance is available from the Payments Association, see Annex 10**.**

Annex 3. Life cycle of certificates

The applicability of the PCI SSC regulation in combination with the supplementary requirement (of periodic reassessment) has the following consequences. A distinction is made in this respect between PCI+ POI devices (the so-called installed base) and new POI devices.

Installed base terminals.
The rules for existing **PCI+ 1.3 terminals** are as follows:

1. PCI+ 1.3 POI devices may no longer be sold and connected to the payment infrastructure.
2. A five-year maintenance period came into effect on 30 April 2014 for most of the PCI+ 1.3 terminals, with the exception of a limited number of terminals for which the period of use will end before 2019. See the list of approved terminals on the website of the Payments Association.

The rules for existing PCI+ 2.0 POI devices are as follows:

1. PCI+ 2.0 POI devices may be sold and connected to the payment infrastructure until 30 April 2017, which is also the last date on which PCI PED 2.x POI devices may be sold and connected. The Payments Association reserves the right to initiate a re-evaluation (against PCI+ 2.0) during this period as and when appropriate. Afterwards a maintenance period will come into effect.

The following applies to the **new POI devices**:

1. New POI devices must have either a PCI PED 2.x, a PCI PTS 3.x or a PCI PTS 4.x certificate. In addition, the supplier must also have an approval certificate from the Payments Association.
2. POI devices certified against PCI PED 2.x can be sold and connected to the payment infrastructure until 30 April 2017. The Payments Association reserves the right to initiate a re-evaluation during this period as and when appropriate. Afterwards a maintenance period will come into effect.
3. POI devices certified against PCI PTS 3.x can be sold and connected to the payment infrastructure until 30 April 2020. The Payments Association reserves the right to initiate a re-evaluation during this period as and when appropriate. Afterwards a maintenance period will come into effect.
4. POI devices certified against PCI PTS 4.x can be sold and connected to the payment infrastructure until 30 April 2023.The Payments Association reserves the right to initiate a re-evaluation during this period as and when appropriate. Afterwards a maintenance period will come into effect.

A generic maintenance periods of 5 years apply, unless a sunset date is issued by the card schemes for the brands which are accepted on the POI[1]. See the list of approved POI devices for the actual maintenance periods.

[1] In 2013 VISA EU issued a sunset date for PCI 1.x certified POI's. Same time they announced the intention to do this later for PCI 2.x device as well.

Annex 4. Template for Certificate of Conformity for POI hardware

The undersigned,

<company name>, based in <postcode>, <place>, <visiting address>,
legally represented in this matter by <name>,
hereafter referred to as: Supplier

Whereas:

- Supplier signed the Standard agreement for POI device suppliers with the Payments Association on ….;
- …. [enter the objective of this statement ..]

Declares the following in addition to the Standard agreement for POI device suppliers:

1. For Acquirers who are members of the Dutch Payments Association (hereafter: the Payments Association), Supplier will only use POI devices with an approval certificate of the Payments Association in accordance with the type submitted for certification. The POI device with serial number <> was presented to the Payments Association as a reference device.
2. Supplier agrees that the reference device submitted will be stored by the Payments Association for as long as the POI device continues to play an active role in the flow of payments. The reference device remains the property of the Supplier.
3. Supplier is responsible for any parts bought from third parties. In order to carry this responsibility, the Supplier has entered into agreements with his own suppliers or with the parties that he is buying from.
4. Any changes to the POI device or in the POI device's production process - in relation to the applicable security measures - will be submitted to the Payments Association for evaluation in good time. The modification(s) in conformity with the submitted request will not be implemented before the Payments Association has given its approval in writing.
5. Any loss arising from non-compliance with this Certificate of Conformity must be borne by the Supplier.

Place ..... date .....

For < Supplier >

Name:
Title

Annex 5. Template for Certificate of Conformity for POI software

The undersigned,

<company name>, based in <postcode>, <place>, <visiting address>,
legally represented in this matter by <name>,
to be called hereafter: Supplier

Whereas:

- Supplier signed the Standard Agreement for POI device suppliers on .....
- …. [enter the objective of this statement ..]

Declares the following in addition to the Standard Agreement for POI device Suppliers:

1. For Acquirers who are members of the Dutch Payments Association (hereafter: the Payments Association), Supplier will only use security software certified - or in the event of a small modification, still to be certified - by the Payments Association. If the certified security software provides SRED, SRED must be deployed.
2. The most recently certified security software version has the following characteristics:
   - Details of the evaluation report: <Title, version, date E-lab>
   - <Sha-1|Sha-2> HASH calculated on the source code as indicated in the evaluation report.
   - Description of Build environment:
     - Operating system, Service Pack| Patch level, etc.;
     - Supplier, version numbers, etc. Build environment compiler, etc. (sufficient information to construct the Build environment from scratch)
   - <Sha-1|Sha-2> HASH calculated on the resulting binary and/or compilation result.
3. Only applicable in the case of small modifications:
   - Details of the release note: <Title, version, date>
   - Risk analysis, to be performed by supplier to substantiate or associated with the modification, § release note or separate document.
   - <Sha-1|Sha-2> HASH calculated on the source code as indicated in the release note.
   - Optional if it is the same as point 2
     [Description of Build environment:]
     - Operating system, Service Pack| Patch level, etc.;
     - Supplier, version numbers, etc. Build environment compiler, etc.
     - Etc. (sufficient information to construct the Build environment from scratch)
   - <Sha-1|Sha-2> HASH calculated on the resulting binary and/or compilation result.

4. Supplier agrees that the source code will be stored by the Payments Association or by a designated external party (escrow, evaluation lab) for as long as the POI device continues to play an active role in the flow of payments. The source code remains the property of the Supplier.
5. Supplier is responsible for ensuring that the components required to arrive from the certified source code to the recorded binary and/or compilation results, remain available.
6. Any modifications to the security software - in relation to the applicable security requirements - will be submitted in time to the Payments Association.
7. Major modifications in the security software will not be implemented until the Payments Association has given its written approval.
8. Small modifications can be implemented after the Payments Association has been informed, by means of Release notes (at the latest within one year, otherwise subject to certification).
9. Any loss arising from non-compliance with this Certificate of Conformity must be borne by the Supplier.

Place ..... date .....

For < Supplier >

Name:
Title

Annex 6. Template for Certificate of Conformity for Payment Chain <POI>

The undersigned,
The undersigned,

<company name>, based in <postcode>, <place>, <visiting address>,
legally represented in this matter by <name>,
to be called hereafter: Supplier

Whereas:

- Supplier signed the Standard Agreement for POI device suppliers on .....
- …. [enter the objective of this statement ..]

Declares the following in addition to the Standard Agreement for POI device Suppliers:

1. For Acquirers who are members of the Dutch Payments Association (hereafter: the Payments Association), Supplier will only connect certified POI devices to the payment chain described below.
2. The payment chain - from the POI device to the transaction-processing systems of the acquirer processor used by one or more Acquirers of the Dutch Payments Association - is composed of the following elements (This concerns elements ranging from a card reader to servers that provide access to sensitive card data and/or key material with which the card data and/or PIN is protected):
   i) <EPP|PED>
   ii) [Card reader, in the case of unattended POI devices]
   iii) [Concentrator/Front-end processor]
   iv) [HSM]
   v) Acquirer processor

< Please include a sketch that outlines the payment chain >

3. The chain elements referred to in Point 2 satisfy the following security standards: <PCI PTS, PCI DSS, PCI PA-DSS, PCI HSM, PCI PIN> (specify element for each chain)

4. The following Point-to-Point encryption method is used between the chain elements referred to in Point 2:
   <For example: The payment chain from 2i to 2v uses SRED and S-UKPT in accordance with the C-Tap 10 specifications
   - or –
   The payment chain from 2i to 2ii uses SRED; from 2i to 2ii uses Three-key Triple DES DUKPT; from 2ii to 2v uses S-UKPT in accordance with the C-Tap 3 specifications>
5. Any modifications to the payment chain - in relation to the applicable security requirements - will be submitted in time to the Payments Association.
6. Any loss arising from non-compliance with this Certificate of Conformity must be borne by the Supplier.

Place ..... date .....

For < Supplier >

Name:
Title

Annex 7. Certification of non-PED POI devices

1. General

The security certification of POI devices is largely focused on the security module which is required when using a PIN as authentication method for an electronic payment transaction.
Market developments have ensured that POI devices will be available without support of PIN entry The regulations of the Global Brands allows this.
Because these terminals have a different (security) risk profile, for these non-PED POI devices a different certification process will be used.

2. Requirements

There is a secure protocol required for communication between the Acquirer host and the POI device in the case of non-PED terminals. The secure protocol must guarantee mutual authentication and secure messaging between POI device and Acquirer host. This also assumes a solid payment application. It is the responsibility of the acquirer (processor) to specify the security protocol and to implement it.

It is then up to the supplier of the POI device to support the security protocol in a safe way. For example, secret keys (according to generally accepted ISO security standards) may not appear in clear text in unprotected memory of the POI device.

The applicable international requirements are included in the SEPA Cards Standardisation Volume version 7.0. The following requirements apply in addition to the SRED obligation: I2, I3, I4, K9 and K17.

3. Procedure

(a) registration

To monitor the deployment of non-PED POI devices, the supplier of the POI device must register (including the conclusion of an Agreement) at the Payments Association referring to the security and functional certifications this POI device has gone through.

(b) review

In case of a CTAP-TSC certified POI device it can be assumed that the POI device will support secure communication (including mutual authentication) with the acquiring host. In case of other terminals (e.g. IFSF, CTAP SSL3/TLS-only) this must be seen in a form of (acquiring) certification. In the absence of a CTAP TSC certificate it is up to the supplier to prove that the POI device has implemented the required security protocol in a safe manner. For this category of POI devices this may be demonstrated on the basis of design-(and test) documentation. The documentation will be reviewed by the Payments Association. If there is any reason, the Payments Association reserves the right to have the documentation validated by an external laboratory. If it is insufficient demonstrated that the POI device has implemented the security protocol in a safe way and there are risks, this is indicated to the acquirer. The Payments Association shall, in consultation with the

acquirer, determine which mitigation measures can be taken to guarantee the security of the payment chain.

(c) Lifecycle and approval

Finally, the supplier receives from the Payments Association an admission letter where the approval period is indicated. This period will be equal to the POI devices with PIN use, where the periodic reassessment will lapse.

Annex 8. Privacy Shield assessment procedure

If a POI device is integrated in a vending machine, the “EPC343-08 PRIVACY SHIELDING FOR PIN ENTRY” Version 1.4 of 30 September 2009 must be satisfied.

This assessment can be performed by one of the accredited labs or by the Payments Association. This assessment can be performed by taking the measurements according to an initial reference item. Based on technical drawings it is also possible to use the measurements to determine whether the standard has been met. The 5 key is the reference point for determining the height of the privacy shield and for determining the installation height, calculated from the ground to the centre of the 5 key. For this purpose we would like to receive the measurements of the installation frame in combination with the certified POI device (preferably CAD drawings in PDF format) and the vending machine.

If it finds itself in agreement, the Payments Association will inform the supplier in writing. The approval certificate is issued on condition that the supplier issues a certificate of conformity. With this certificate, the supplier undertakes that the POI device will only be commissioned in the operational environment with the security-relevant components that were assessed. The certificate of conformity must cover both hardware and placement aspects (see Annex 9).

Annex 9. Certificate of Conformity for Installation Method <POI>

The undersigned,

<company name>, based in <postcode>, <place>, <visiting address>,

legally represented in this matter by <name>,

to be called hereafter: Terminal Supplier

Declares the following:

1. The Terminal Supplier, in order to ensure application for the Dutch market in accordance with the standard:
   - EPC343-08 Version 1.4 approved 30 September 2009, PRIVACY SHIELDING FOR PIN ENTRY

   will supply the assessed <terminal model name> as offered by him for assessment <reference to drawing and measurements>.

2. Any modifications to the <terminal model name> affecting the guidelines as described in the *standard* will be submitted in time to the Dutch Payments Association. The modifications in conformity with the submitted request will not be implemented until the Dutch Payments Association has given its approval in writing.

3. Any loss arising from non-compliance with this Certificate of Conformity must be borne by the Terminal Supplier.

Place ..... date .....

For < Terminal Supplier>

Name:

Title

Annex 10. Contact information

Registration

Betaalvereniging Nederland / Dutch Payments Association

Visiting address: Beethovenstraat 300 , 1077 WZ Amsterdam
PO Box 83073, 1080 AB Amsterdam

Contacts: Mr O Covers, Mr R. Steenbeeke.

Telephone: +31 20 305 1900
Fax: +31 20 305 1912
E-mail: o.covers@betaalvereniging.nl, r.steenbeeke@betaalvereniging.nl
website: www.betaalvereniging.nl

Accredited evaluation labs
The Payments Association accepts investigations performed by the following research organisations:

Brightsight BV
Delftechpark 1
2628 XJ Delft

Telephone: +31 15 269 2500
Fax: +31 15 269 2555
E-mail: marrewijk@itsef.com
Website: www.brightsight.com

T-Systems GEI GmbH
Vorgebirgsstrasse 49,
D-53119 Bonn
Germany

Telephone: +49 228 9841 114
Fax: +49 228 9841 60
E-mail: robert.hammelrath@t-systems.com
Website: http://www.t-systems.de/ict-security

Security Research & Consulting GmbH
Graurheindorfer Strasse 149a
53117 Bonn
Germany

Telephone: +49 228 2806 101
E-mail: detlef.kraus@src-gmbh.de
Website: www.src-gmbh.de

TÜV Informationstechnik GmbH
PO Box 103261
45032 Essen
Mr F. Beuting

Annex 11. Glossary

ATM	Automated Teller Machine
BEA	POI device (*BetaalAutomaat*)
CIM	Contract Information Manager, the system in which the processing contacts are stored. This primarily concerns the technical parameters arising from the Contract between the Merchant and the Acquirer, which are established for each terminal and for each brand.
CTAP	Common Terminal Acquirer Protocol. CTAP is a multi-host, multi-acquirer payment infrastructure and architecture for the processing of Point-of-Sale transactions.
Debit	The method of electronic payment in which the amount to be paid is immediately debited from the account of the card holder. In the context of this risk analysis this refers to payment by means of the magnetic strip plus PIN.
ECB	European Central Bank
EPC	European Payment Council - established in 2002. The EPC calls itself "the decision-making and coordination body of the European banking industry in relation to payments." The primary task of the EPC is the development of the Single Euro Payments Area. The 74 members are banks and associations of banks.
EMV	Europay, MasterCard and Visa, developers and owners of the protocol.
GEA	ATM (*GEldAutomaat*)
IFSF	International Forecourt Standards Forum – a European organisation that develops standards for the connection of devices on service station forecourts, such as dispensers, Tank Level Gauges, Price Signs, Car Washes and Outdoor POI devices. As well as POI devices in the Petroleum sector, IFSF can also be used by terminal suppliers for parking solutions and sub post offices.
LoA	Letter of Approval
Maestro	MasterCard product for merchant payments by debit card.
NAI	Nederlands Arbitrage Instituut, stands for - Dutch Arbitration Institute - for handling disputes relating to the assessment of a terminal by the Payments Association Netherlands.
PAN	Primary Account Number. 14 or 16-digit numerical code encoded in the EMV chip and on the magnetic strip (embossed on the front in the case of a Credit Card). The PAN is a composite number whose first 6 digits are the Issuer Identification Number (IIN) of the card issuer. The first part of the IIN is the Major Industry Identifier (debit cards therefore always start with a 3, 4, 5, or 6). This is followed by the individual account identifier of the card holder, as well as a check digit that checks the authenticity of the PAN.
PCI	Payment Card Industry
PCI-EPP	Payment Card Industry – Encrypting PIN Pad (standard)
PCI-PTS	Payment Card Industry – PIN Transaction Security (standard). For PCI version 1.3 and 2.1, the collective name for the various PCI programs such as EPP, PED, UPT and HSM. PCI PTS version 3 refers to a Point of Interaction (POI) to describe the architectures mentioned above.

PIN	Personal Identification Number. Established term for paying by debit.
POI	Point of Interaction
POS	Point of Sale
SRED	Secure Reading and Exchange of Data - is part of the PCI PTS standard to protect card data immediately after reading.
TMS	Terminal Management System
TSC	Terminal Secure Component. - TSC Certificate – the TSC Certificate is unique and is used for the key relationship between POI device and the transaction-processing host. A certificate links a public key to a particular unique name.
Unattended POI device	The card holder performs the transaction independently, without the involvement of a cashier. Examples are POI devices integrated in: vending machines, ticket machines, self-service terminal, etc.
V PAY	Visa product for merchant payments by debit card.