PBS A/S
Lautrupbjerg 10
P.O. 500
DK – 2750 Ballerup

T +45 44 68 44 68
F +45 44 86 09 30
pbsmailservice@pbs.dk
www.pbs.dk

PBS-nr. 00010014
CVR-nr. 20016175

Declaration for key loading

Table of contents

1 Declaration

As a supplier of key loading of payment terminals and PIN entry devices operated by PBS we hereby declare that we are aware of and accept to observe the security requirements for key loading stated below.

We confirm to be compliant with these security requirements and with related regulations as set up by Visa and MasterCard.

We also confirm to be in compliance with the conditions of approval stated below

_____ _____

Date – signature – company stamp

2 Conditions for approval

In order to be approved and to be added to the PBS A/S' list of certified suppliers, the supplier must sign this declaration thereby acknowledging the comprehension of and willingness to comply with these security requirements.

The supplier is not allowed to distribute terminals and/or PIN pads until an initial inspection of the supplier's premises and security measures has been carried out by an auditor from PBS A/S.

If the security of the supplier's plant, procedures, or systems varies from the standards in this document, but in the judgement of the auditor, is equal or superior to these standards, the supplier is considered being in compliance with the provisions of this declaration.

If the auditor finds that the supplier is not compliant with this declaration, the auditor will make a new inspection within 60 days. If, at that time, the supplier is still not in compliance, the supplier will either not be added to or removed from the approved supplier list until the supplier is found compliant.

After the initial approval an auditor from PBS A/S is at any time entitled to make follow up inspections at the manufacturing and key loading premises in order to confirm, that the supplier continuously is compliant with to the provisions stipulated in this declaration and in other guidelines stipulated by PBS A/S.

When the auditor has completed the inspections, a draft report will be issued for the supplier to comment on. The final version – including the supplier' comments – will be issued and distributed to the parties.

3 Security requirements

3.1 General Requirements for Key loading Facilities

Key loading of PIN Entry Devices (PIN-pads) must take place within security controlled areas with controlled and restricted access. The purpose of such restrictions and controls is to prevent non-authorised viewing of secure operations and/or sensitive data.

The supplier has to define the authority levels and entry criteria's for the secure loading areas.

Access to these secure areas is to be limited to a minimum and to be controlled on a formal basis with vetting for the authorized employees involved, and strict escorting of any others.

Use of secure data shall only be permitted in secured areas. Secure data comprises all records and all media containing secret data including paper and computer disk files.

The transmission or shipment of secure data or products containing secure data shall be encrypted with assurance of complete, timely receipt.

An employee should be appointed as responsible for all security matters including follow up upon log registrations. This employee should also perform regular tests and follow up on the adequacy and compliance of security rules and procedures.

3.2 Subcontractors

When using subcontractor(s) the subcontractor must be fully compliant with the requirements stipulated in this declaration and the subcontractor must be approved by PBS before usage is initiated.

The supplier is responsible for all deliveries from the subcontractor in the same way, as the supplier is responsible for own deliveries.

In case of subcontracting, adherence to security requirements shall be included in the terms and conditions of the agreement with the subcontractor.

3. Personnel, visitors and confidentiality

The supplier must implement security procedures, which apply to all employees as well as consultants and guard service personnel (internal as well as external).

Adherence to security requirements shall be included in the terms and conditions of all employees working in the security controlled area.

All information concerning the manufacture and key loading of PIN-pads must be treated confidentially by the supplier and all employees. All employees taking part in the key loading processes must sign a secrecy declaration concerning these matters.

Visitors, service and maintenance personnel may be admitted to the key loading area only when escorted by an authorized employee during the entire stay. The access must be granted by the manager responsible for key loading and only when a positive identification has been established.

A visitor's log must be maintained with the visitors name, company name, purpose of the visit, name and signature of hosting employee and time of arrival and departure.

3.3 Physical security for the key loading premises

The key loading premises must be located in an area served by public law enforcement and by fire protection services. The key loading area must be adequately secured with an intrusion alarm system with auxiliary power capability to ensure operation in the event of a central power failure. The alarm system must be directly connected to the police and/or a recognized security company.

The alarm system may consist of vibration alarms, magnetic contact detectors or similar security measurements against intrusion.

Access to the key loading area must be restricted to authorised personnel only. The area must be protected by an access control system with an in and out card reader system connected to a central computer which monitors and logs all movements of staff and visitors. Log registrations are to be kept for 1 year.

Access shall only be possible via the combined use of card reader and entering an individual PIN, or similar, for instance biometrics.

Access to the loading area is to be camera monitored and the recordings to be stored for at least 3 months, unless otherwise restricted by law.

If access to the key load area is dependent on the use of physical keys, for instance in emergency situations, such keys should be kept in a secured key safe under the dual supervision of the employees responsible for security. The usage of such keys is to be registered in a log.

3.4 Securing PIN-pads and loading equipment

Only PIN-pads approved by PBS A/S may be loaded with Dankort and Visa/Dankort keys. A list of approved crypto modules and of approved suppliers of terminals accepting Dankort and Visa/Dankort can be found on www.dankort.dk.

The supplier must ensure that all PIN pads and components are securely stored at any time and protected against substitution, tampering and theft prior to, during and after key load.

The loading equipment must be placed within the secure area at all time and without being connected to Local Area Network (or similar) or the Internet.

When not in use for key load the equipment must be securely stored in a safe or similar. The equipment shall not be accessible for non-authorised personnel. The equipment must be protected to prevent any type of monitoring that could result in the unauthorized disclosure of any component and must always handled under dual control.

Activating the loading equipment for key load shall only be possible under dual control and by using individual passwords or similar security. The passwords shall be allocated to authorised personnel only and must be changed on a regular basis.

The activation of the loading equipment must be logged with information on activation time and names of authorized personnel performing the activation.

The loading equipment must be tamper responsive and must ensure that keys are overwritten after usage. When shut down, the loading equipment shall erase any stored secure data.

When idle (for more than 15 minutes), the loading equipment shall shut itself down and thereby erase any secure data stored in the said equipment.

3.5 Handling and loading security for cryptographic keys

Secret and private encryption keys must be transmitted in a secure manner and never exist outside a Tamper Resistant Security Module, unless encrypted or securely stored and managed, using the principles of dual control and split knowledge. No single employee must ever be able to access or use all components of a single cryptographic key.

Key parts must be stored in individual compartments in a safe and in tamper evident envelopes (or equivalent) under the responsibility of different authorized key custodians and must never be stored together.

Procedures must exist and be demonstrably in use to replace any known or suspected compromised key and its subsidiary keys (those keys enciphered with the compromised key) to a value not feasibly related to the original key.

The loading of keys or key components must incorporate a validation mechanism such that the authenticity of the keys is ensured and it can be ascertained that they have not been tampered with, substituted or compromised.

Logs must be kept for any time that keys, key components, or related materials are removed from storage and/or loaded into a TRSM.

The key loading process has to be logged, as a minimum showing time and date for the key loading, the number and individual identity of PIN-pads loaded and the unambiguous identity of the key custodians and other employees involved in key handling and loading.

Secret and private keys and key components that are no longer used or needed must be securely destroyed, e.g. by shredding of paper or overwriting of computer files.

3.6 Documentation of procedures and security

Documented procedures must be established and must be demonstrably in use for all key-loading activities. This applies also for the security requirements and how they are implemented. The documentation should include physical security, alarm systems, monitoring, logging, segregation of duties and access control.

All key management processes and procedures must be fully documented. This includes key generation, key distribution, key storage, destruction of old keys, split knowledge and dual control of keys (so that it requires 2 or 3 people, each knowing only their part of the key, to reconstruct the whole key), prevention of unauthorised substitution of keys, replacement of known or suspected compromised keys and the duties and responsibilities of the key custodians.

The documentation – which should be distributed to all relevant employees – must be updated at any time.

3.7 Product storage and inventory

The supplier shall be able to account for the number and location of all PIN pads prior to, during and after key loading. This applies also for sample PIN pads. Until shipment, the packed PIN pads shall be kept in a secured area.

When key loading is completed the PIN pads should be individually boxed and a tamperproof seal applied to the box to make it evident if the package subsequently has been tampered with or attempted to. Equivalent methods of preventing tampering or making tampering attempts clearly visible may be used.

If tamper proof seals are used they must be securely stored and strictly accounted for.

If there is evidence - or indications - of tampering the PIN-pad(s) must be shipped. The supplier shall ascertain the cause of the tamper and take the appropriate steps.

The packed PIN-pads should be accompanied by security guidance's for the customers describing their actions to be taken in case of tampering or suspicion of tampering or other security breaches.

3.8 Notification to PBS A/S in case of insufficient security

The supplier must notify PBS A/S immediately if any circumstances in the company imply that the requirements in this declaration are not or have not been met.

The supplier shall immediately report to PBS A/S the suspected or confirmed loss of any PIN-pads that are lost, stolen, or missing from the manufacturer's possession while in route.

3.9 Minimum Shipping Security Standards

Approved methods for shipping unloaded PIN pads to the initial key loading facility are when shipped and stored in tamper evident packaging or shipped and stored containing a secret that is immediately and automatically erased if the item is tampered with. The secret shall be verifiable by the initial key loading facility only, but not feasibly possible to be determined by unauthorized parties.

3.10 Changes to the provisions of this declaration

PBS A/S may at any time change the provisions of the declaration with a reasonable period of notice.

In case of minor (editorial) changes to the declaration, PBS A/S will forward a new declaration, which the supplier/manufacturer must sign and return to PBS A/S before the stipulated deadline by which the supplier/manufacturer must meet new requirements.

In case of substantial changes to the declaration, PBS A/S will undertake a period of consultation with suppliers/manufacturers before they must meet the new requirements.

3.11 Annual management declaration

The management of the supplier certified by PBS A/S must annually forward a declaration, to PBS A/S in order to confirm still being compliant with the security requirements in this declaration and that they have been met in the preceding calendar year.