Key load security Requirements and Self Assessment form concerning the key loading of chip terminals operated by PBS

Index

List of changes

Date	Version	Description	Page
March 2007	1.0	New document based on Vendor Declaration for Key load	

1. Overview

1.1 Purpose of the questionnaire

This document is intended for evaluating the key loading facilities, procedures and security precautions for the key load of chip terminals operated by PBS. The requirements and the self assessment form is to be used prior to both initial inspection of the key load facilities and also prior to subsequent regular inspections.

When the form has been filled in it must be returned to The PBS Internal Audit Department and it will later provide the basis for the inspection carried out by PBS Internal Audit.

1.2 How to Complete the Questionnaire

The questionnaire is divided into 10 sections. Each section focuses on a specific area of security, based on the requirements to be fulfilled before inspection and audit of the key load premises may be initiated. For any questions where N/A is marked, a brief explanation should be attached.

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.

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.

13 Questionnaire Reporting

The following must be included with the self assessment questionnaire:

1.2.1 Organization Information

Corporate name:		?:	
Contact name:		Title:	
Phone:		E-mail:	

1.2.2 List all Subcontractors

Corporate name:		?:	
Contact name:		Title:	
Phone:		E-mail:	

1.2.3 List HSM software/hardware in use

1.4 Rating the Assessment

After completing each section of the assessment, users should fill in the rating boxes as follows:

In each section IF…	THEN, the section rating is …
ALL questions are answered with "yes" or "N/A"	**Green** - The manufacturer is compliant with the self assessment portion of the Questionnaire. *Note: If "N/A" is marked, attach a brief explanation.*
ANY questions are answered with "no"	**Red** – The manufacturer is not considered compliant. To reach compliance, the risk(s) must be resolved and the self assessment must be retaken to demonstrate compliance.

Section 1:	Green Red	Section 6:	Green Red	Section 11:	Green Red
Section 2:	Green Red	Section 7:	Green Red		
Section 3:	Green Red	Section 8:	Green Red		
Section 4:	Green Red	Section 9:	Green Red		
Section 5:	Green Red	Section 10:	Green Red		

Overall Rating: Green Red

2. General requirements for PED manufacturing and key loading facilities

2.1	Requirements
2.1.1	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.
2.1.2	The supplier has to define the authority levels and entry criteria's for the secure loading areas.
2.1.3	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.
2.1.4	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.
2.1.5	The transmission or shipment of secure data or products containing secure data shall be encrypted with assurance of complete, timely receipt.
2.1.6	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.

2.2	Questions	Response		
2.2.1	Is the area for loading of PED keys security controlled?	☐ Yes	☐ No	
2.2.2	Is access to the area restricted and controlled?	☐ Yes	☐ No	☐ N/A
2.2.3	Are authority levels defined?	☐ Yes	☐ No	
2.2.4	Are entry criteria defined?	☐ Yes	☐ No	
2.2.5	Is access limited to a minimum?	☐ Yes	☐ No	

2.2.6	Is access controlled on a formal basis with vetting for the authorized employees involved?	☐ Yes	☐ No	
2.2.7	Is access controlled with strict escorting of any others?	☐ Yes	☐ No	☐ N/A
2.2.8	Is use of secure data permitted in secured areas, only?	☐ Yes	☐ No	
2.2.9	Is transmission and shipment of secure data or products containing secure data encrypted with the assurance of complete, timely receipt?	☐ Yes	☐ No	☐ N/A
2.2.10	Is an employee appointed as responsible for all security matters including follow-up upon log registrations?	☐ Yes	☐ No	
2.2.11	Does the security responsible perform regular tests and follow-up on the adequacy and compliance of security rules and procedures?	☐ Yes	☐ No	

3. Subcontractors

3.1	**Requirements**
3.1.1	When using sub-contractor(s) the sub-contractor must be fully compliant with the requirements stipulated in this declaration and the sub-contractor must be approved by PBS before usage is initiated.
3.1.2	The supplier is responsible for all deliveries from the sub-contractor in the same way, as the supplier is responsible for own deliveries.
3.1.3	In case of subcontracting, adherence to security requirements shall be included in the terms and conditions of the agreement with the sub-contractor.

3.2	Questions	Response		
3.2.1	Does key loading involve any sub-contractor(s)?	☐ Yes	☐ No	
3.2.2	Is the sub-contractor audited for being compliant with the requirements in this document?	☐ Yes	☐ No	☐ N/A
3.2.3	Is the sub-contractor approved by PBS?	☐ Yes	☐ No	☐ N/A
3.2.4	Does the agreement with the sub-contractor include conditions of adherence to the security requirements in this document?	☐ Yes	☐ No	☐ N/A

4. Personnel, Visitors and Confidentiality

4.1	Requirements
4.1.1	The supplier must implement security procedures, which apply to all employees as well as consultants and guard service personnel (internal as well as external).
4.1.2	Adherence to security requirements shall be included in the terms and conditions of all employees working in the security controlled area.
4.1.3	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.
4.1.4	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.
4.1.5	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.

4.2	Questions			
4.2.1	Do security procedures apply to all employees as well as consultants, and guard service personnel (internal as well as external)?	☐ Yes	☐ No	
4.2.2	Is adherence to security requirements included in the terms and conditions of all employees working in the security controlled area?	☐ Yes	☐ No	
4.2.3	Have all employees taking part in the key loading processes signed a confidentiality declaration?	☐ Yes	☐ No	☐ N/A
4.2.4	Are visitors, service and maintenance personnel admitted to the key loading area escorted by an authorized employee during the entire stay?	☐ Yes	☐ No	☐ N/A
4.2.5	Is the access granted by the manager responsible for key loading?	☐ Yes	☐ No	
4.2.6	Is the access granted when a positive identifications has been established, only?	☐ Yes	☐ No	☐ N/A
4.2.7	Is the visitor log maintained with the visitor's name, company name, purpose of the visit, signature of the visitor, signature of the hosting employee, and times of arrival and departure (entering/exiting the key loading area)?	☐ Yes	☐ No	☐ N/A

5. Physical security for the key loading premises

5.1	Requirements	Response
5.1.1	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.	
5.1.2	The alarm system may consist of vibration alarms, magnetic contact detectors or similar security measurements against intrusion.	
5.1.3	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.	
5.1.4	Access shall only be possible via the combined use of card reader and entering an individual PIN, or similar, for instance biometrics.	
5.1.5	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.	
5.1.6	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 supervision of the employee responsible for security. The usage of such keys is to be registered in a log.	

5.2	Questions	Response		
5.2.1	Are the key loading premises located in an area served by public law enforcement?	☐ Yes	☐ No	
5.2.2	Are the key loading premises located in an area served by fire protection services?	☐ Yes	☐ No	
5.2.3	Are the key loading premises secured with an intrusion alarm system?	☐ Yes	☐ No	
5.2.4	Is the intrusion alarm system equipped with an auxiliary power capability to ensure operation in the event of a central power failure?	☐ Yes	☐ No	
5.2.5	Is the alarm system connected directly to the police?	☐ Yes	☐ No	
5.2.6	Is the alarm system connected directly to a recognized security company?	☐ Yes	☐ No	
5.2.7	Is access to the key loading area restricted to authorized personnel only?	☐ Yes	☐ No	
5.2.8	Is the area protected with an in/out card reader system connected to a central computer which logs all movements of staff and visitors?	☐ Yes	☐ No	☐ N/A
5.2.9	Are the log registrations kept for 1 year?	☐ Yes	☐ No	☐ N/A
5.2.10	Is access only possible via the combined use of the card reader and entering of an individual PIN, or similar, or e.g. biometrics?	☐ Yes	☐ No	☐ N/A
5.2.11	Is the access to the key loading area under camera surveillance?	☐ Yes	☐ No	☐ N/A
5.2.12	Are the camera recordings stored for at least 3 months, unless otherwise restricted by law?	☐ Yes	☐ No	☐ N/A
5.2.13	Is access to the key loading area possible using physical keys? E.g. in emergency situations.	☐ Yes	☐ No	☐ N/A

5.2.14	Are physical keys for access to the key load area kept in a secured key safe under dual surveillance of the employees responsible for security?	☐ Yes	☐ No	☐ N/A
5.2.15	Is the use of such physical keys registered in a log?	☐ Yes	☐ No	☐ N/A

6. Securing PEDs and key loading equipment

6.1	Requirements
6.1.1	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.
6.1.2	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.
6.1.3	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.
6.1.4	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.
6.1.5	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.
6.1.6	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.

6.1.6	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.

6.2	Questions	Response		
6.2.1	Is the PED to be key loaded approved by PBS?	☐ Yes	☐ No	
6.2.2	Are all PEDs and components securely stored at any time?	☐ Yes	☐ No	
6.2.3	Are all PEDs and components securely protected against substitution prior to, during, and after key load?	☐ Yes	☐ No	☐ N/A
6.2.4	Are all PEDs and components securely protected against tampering prior to, during, and after key load?	☐ Yes	☐ No	☐ N/A
6.2.5	Are all PEDs and components securely protected against theft prior to, during, and after key load?	☐ Yes	☐ No	☐ N/A
6.2.6	Is the key loading equipment placed within the secure area at all times?	☐ Yes	☐ No	
6.2.7	Is the key loading equipment without connection to a LAN and/or the internet?	☐ Yes	☐ No	☐ N/A
6.2.8	When not in use, is the key loading equipment stored in a safe or similar?	☐ Yes	☐ No	☐ N/A
6.2.9	Is the key loading equipment protected from being accessible for non-authorised personnel?	☐ Yes	☐ No	☐ N/A
6.2.10	Is the key loading equipment protected from any type of monitoring resulting in un-authorized disclosure of any key component?	☐ Yes	☐ No	☐ N/A
6.2.11	Is the key loading equipment activated under dual control?	☐ Yes	☐ No	☐ N/A
6.2.12	Is the key loading equipment activated using individual passwords or similar security?	☐ Yes	☐ No	☐ N/A
6.2.13	Is the activation of the key loading equipment logged with information on activation time and names of authorized personnel performing the activation?	☐ Yes	☐ No	☐ N/A

6.2.14	Are passwords are allocated to authorized personnel, only?	☐ Yes	☐ No	☐ N/A
6.2.15	Are passwords changed on a regular basis?	☐ Yes	☐ No	☐ N/A
6.2.16	Is the key loading equipment tamper responsive?	☐ Yes	☐ No	☐ N/A
6.2.17	Are keys in the key loading equipment overwritten after usage?	☐ Yes	☐ No	☐ N/A
6.2.18	Is any stored secured data erased when the key loading equipment is shut down?	☐ Yes	☐ No	☐ N/A
6.2.19	Does the key loading equipment shut itself down when idle more than 15 minutes?	☐ Yes	☐ No	☐ N/A

7. Handling and loading security for cryptographic keys

7.1	Requirements
7.1.1	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.
7.1.2	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.
7.1.3	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.
7.1.4	Logs must be kept for any time that keys, key components, or related materials are removed from storage and/or loaded into a TRSM.

7.1.5	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.	
7.1.6	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.	

7.2	**Questions**	**Response**
7.2.1	Are secret and private encryption keys transmitted in a secure manner and never existing outside a Tamper Resistant Security Module, unless encrypted or securely stored and managed, using the principles of dual control and split knowledge?	☐ Yes ☐ No
7.2.2	Is any single employee ever able to access or use all components of a single cryptographic key?	☐ Yes ☐ No
7.2.3	Are key parts stored in individual compartments in a safe and in tampered evident envelopes (or equivalent) under the responsibility of different authorized key custodians?	☐ Yes ☐ No ☐ N/A
7.2.4	Do security precautions ensure that key parts are never stored together?	☐ Yes ☐ No ☐ N/A
7.2.5	Do procedures exist and are they demonstrably in use to replace any known or suspected compromised key and its subsidiary keys to a value not feasibly related to the original key?	☐ Yes ☐ No ☐ N/A
7.2.6	Does the loading of keys or key components incorporate a validation mechanism that the authenticity of the keys is ensured and it can be ascertained that they have not been tampered with, substituted or compromised?	☐ Yes ☐ No ☐ N/A
7.2.7	Are logs updated and kept for every time that keys, key components, or related materials are removed from storage and/or loaded into a TRSM?	☐ Yes ☐ No ☐ N/A
7.2.8	Is the key loading process logged?	☐ Yes ☐ No ☐ N/A
7.2.9	Does the log include 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?	☐ Yes ☐ No ☐ N/A

7.2.10	Are secret and private keys and key components that are no longer used or needed securely destroyed, e.g. by shredding of paper or overwriting of computer files?	☐ Yes	☐ No	☐ N/A

8. Documentation of procedures and security

8.1	Requirements
8.1.1	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.
8.1.2	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.
8.1.3	The documentation – which must be distributed to all relevant employees – must be updated at any time.

8.2	Questions	Response
8.2.1	Are documented procedures established and are they demonstrably in use for all key-loading activities?	☐ Yes ☐ No
8.2.2	Does the documentation include physical security, alarm systems, monitoring, logging, segregation of duties, and access control.	☐ Yes ☐ No ☐ N/A
8.2.3	Are all key management processes and procedures fully documented?	☐ Yes ☐ No ☐ N/A
8.2.4	Does the documentation for key management processes and procedures include key generation, key distribution, key storage, destruction of old keys, split knowledge and dual control of keys, prevention of unauthorised substitution of keys, replacement of known or suspected compromised keys, and the duties and responsibilities of the key custodians?	☐ Yes ☐ No ☐ N/A
8.2.5	Does there exist a documented process for document distribution to all relevant employees?	☐ Yes ☐ No ☐ N/A
8.2.6	Does there exist a documented process for document maintenance ensuring updating at all times?	☐ Yes ☐ No ☐ N/A

9. Product storage and inventory

9.1	Requirements
9.1.1	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.
9.1.2	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.
9.1.3	If tamper proof seals are used they must be securely stored and strictly accounted for.
9.1.4	If there is evidence - or indications - of tampering the PIN-pad(s) must not be shipped. The supplier shall ascertain the cause of the tamper and take the appropriate steps.
9.1.5	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.

9.2	Questions	Response
9.2.1	Does the supplier use an accounting system that registers the number and location of all PIN pads (including sample PIN pads) prior to, during and after key loading?	☐ Yes ☐ No
9.2.2	Are the packed PIN pads kept in a secured area until shipment?	☐ Yes ☐ No ☐ N/A
9.2.3	Are the key loaded and completed PIN pads 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?	☐ Yes ☐ No ☐ N/A
9.2.4	Are tamper proof seals securely stored and strictly accounted for?	☐ Yes ☐ No ☐ N/A
9.2.5	Does documented procedures exist that prevents the PIN-pad(s) from being shipped if there is evidence - or indications - of tampering of the PIN-pad(s)	☐ Yes ☐ No ☐ N/A

9.2.6	Does the procedures include that the cause of the tamper is investigated and the appropriate steps taken?	☐ Yes	☐ No	☐ N/A
9.2.7	Are the packed PIN-pads accompanied by a security guidance's for the customers describing their actions to take in case of tampering or suspicion of tampering or other security breaches?	☐ Yes	☐ No	☐ N/A

10. Minimum shipping security standards

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

10.2	**Questions**	**Response**		
10.2.1	Do documented procedures exist that enforces secure methods for shipping unloaded PIN pads to the initial key loading facility?	☐ Yes	☐ No	
10.2.2	Do the procedures include tamper evident packaging?	☐ Yes	☐ No	☐ N/A
10.2.3	Do the PEDs contain a secret that is immediately and automatically erased if the PED is tampered with?	☐ Yes	☐ No	☐ N/A
10.2.4	Is this secret verifiable by the initial key loading facility, only?	☐ Yes	☐ No	☐ N/A

11. Notification to PBS

11.1	**Requirements**
11.1.1	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.
11.1.2	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.

11.2	Questions	Response
11.2.1	Do documented procedures exist that enforces the supplier to notify PBS A/S immediately if any circumstances in the company imply that the requirements in this declaration are not met?	☐ Yes ☐ No
11.2.2	Does documented procedures exist that enforces the supplier to report to PBS A/S immediately the suspected or confirmed loss of any PIN-pads that are lost, stolen, or missing from the manufacturer's possession while in route.	☐ Yes ☐ No

Terms and definitions

Term	Definition
Access control	Measures that limit access to information or information processing resources to those authorized persons or applications.
Audit Log	A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results. Sometimes specifically referred to as a security audit trail.
Authentication	The process of verifying identity of a subject or process.
Authorization	The granting of access or other rights to a user, program, or process
Compromise	An intrusion into a computer system where unauthorized disclosure, modification, or destruction of cardholder data may have occurred.
Dual Control	A method of preserving the integrity of a process by requiring that several individuals independently take some action before certain transactions are completed.
Encryption	The process of converting information into a form unintelligible to anyone except holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption), against unauthorized disclosure.
Firewall	Hardware and/or software that protect the resources of one network from users from other networks. Typically, an enterprise with an intranet that allows its workers access to the wider Internet must have a firewall to prevent outsiders from accessing its own private data resources.
Intrusion detection Systems	An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.
Key	In cryptography, a key is a value applied using an algorithm to unencrypted text to produce encrypted text. The length of the key generally determines how difficult it will be to decrypt the text in a given message.
Monitoring	A view of activity on a network.
Network	A network is two or more computers connected to each other so they can share resources.
Password	A string of characters that serve as an authenticator of the user.

Term	Definition
Policy	Organizational-level rules governing acceptable use of computing resources, security practices, and guiding development of operational procedures.
Procedure	A procedure provides the descriptive narrative on the policy to which it applies. It is the "how to" of the policy. A procedure tells the organization how a policy is to be carried out.
Sanitization	To delete sensitive data from a file, a device, or a system; or modify data so that data is useless for attacks.
Security Officer	The person who takes primary responsibility for the security related affairs of the organization.
Security policy	The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.
Separation of duties	The practice of dividing the steps in a system function among different individuals, so as to keep a single individual from subverting the process.
Server	A computer that acts as a provider of some service to other computers, such as processing communications, file storage, or printing facility.
Tamper-resistance	A system is said to be tamper-resistant if it is difficult to modify or subvert, even for an assailant who has physical access to the system.
Threat	A condition that may cause information or information processing resources to be intentionally or accidentally lost, modified, exposed, made inaccessible, or otherwise affected to the detriment of the organization.
Two-factor authentication	Authentication that requires users to produce two credentials - something they have (e.g., smartcards or hardware tokens), and something they know (e.g., a password). In order to access a system, users must produce both factors.
User ID	A character string that is used to uniquely identify each user of a system.
Vulnerability	A weakness in system security procedures, system design, implementation, or internal controls that could be exploited to violate system security policy.