Security Standards Council®

Standard:	PCI PIN Transaction Security Point of Interaction Security Requirements (PCI PTS POI)
Version:	1.0
Date:	January 2013
Author:	PCI Security Standards Council

Information Supplement:
ATM Security Guidelines

Table of Contents

1 Related Publications

The following ATMIA/GASA, European Payment Council, Microsoft, Trusted Security Solutions, NIST, and PCI standards are applicable and related to the information in this document.

Standard	Source
ANSI X9.24: Retail Financial Services Symmetric Key Management	ANSI
ATMIA/GASA, Best Practice for ATM Transaction Security	ATMIA/GASA
ATMIA/GASA Best Practices for ATM Cyber Security	ATMIA/GASA
ATMIA/GASA Best Practices PIN Security & Key Management recommendation	ATMIA/GASA
ATMIA/GASA, ATM lifecycle Security Manual, International minimum security guidelines	ATMIA/GASA
ATMIA, ATM Software Security Best Practices Guide	ATMIA
Guidelines for ATM Security	European Payment Council DTR 413
Recommended ATM anti-skimming solutions within SEPA	European Payment Council Doc115-8
ISO 11568: Banking – Key Management (Retail)	ISO
Microsoft Windows XP-based ATM Security Design A solution for secure, well-managed ATMs using Windows XP and Active Directory	Microsoft
Microsoft Managing Windows XP-based ATMs Using SMS and MOM A solution for secure, well-managed ATMs using Windows XP, Active Directory, Systems Management Server, and Operations Manager	Microsoft
Microsoft Windows XP-based ATM Security Design	Microsoft
Microsoft Active Directory Design for Windows XP-based ATMs A solution for secure, well-managed ATMs using Windows XP and Active Directory	Microsoft
2009 Update: Remote Key Loading	Trusted Security Solutions
Guidance for securing Microsoft Windows XP systems for IT Professionals	NIST
Wireless Management and Security — Part 1: General Requirements	NIST
Wireless Management and Security — Part 2: ATM and POS	NIST
Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures	PCI SSC
Payment Card Industry Payment Application Data Security Standard	PCI SSC

Standard	Source
Requirements and Security Assessment Procedures	
Payment Card Industry PTS POI Modular Security Requirements	PCI SSC
Payment Card Industry PTS POI Derived Test Requirements	PCI SSC
Payment Card Industry PIN Security Requirements	PCI SSC

***Note**: These documents are routinely updated and reaffirmed. The current versions should be referenced when using these requirements.*

2 Introduction

2.1 Document Purpose and Scope

This document proposes guidelines to mitigate the effect of attacks to ATM aimed at stealing PIN and account data. These guidelines are neither definitive nor exhaustive and are not intended to be used as requirements for a validation program at the PCI SSC.

For additional information regarding any compliance questions, contact the payment brand(s) of interest.

2.2 Intended Audience

This Information Supplement is intended for ATM manufacturers, integrators, and deployers of ATMs.

2.3 Terms and Acronyms

Term/Acronym	Description
AC	ATM controller
ATM compromise	A violation of the security of a system such that an unauthorized disclosure of sensitive information may have occurred. This includes the unauthorized disclosure, modification, substitution, or use of sensitive data (including plaintext cryptographic keys and other keying material).
ATM Fraud	The illegal procurement of cash, money value or cardholder information via ATM networks
EPP	Encrypting PIN PAD, a tamper-responsive security device that provides secure PIN entry and storage of cryptographic material. It is designed to be integrated into ATMs or self-service POS terminals.
Fascia	ATM front, available for user cardholder interaction: It normally includes the devices required for cardholder interface, such as the (secure) keypad, the card-reader slot or the NFC-device reader, the screen etc. It may also include the note-dispensing tray; the deposit-taking compartment, etc.
NFC	Near Field Communication Standards that enable payment applications to communicate with terminals by being in close proximity with a reading pad in the terminal.

Term/Acronym	Description
PCI DSS	PCI SSC Data Security Standard The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.
PCI PA-DSS	PCI SSC Payment Application Data Security Standard This document is to be used by Payment Application-Qualified Security Assessors (PA-QSAs) conducting payment application reviews; so that software vendors can validate that a payment application complies with the PCI DSS Payment Application Data Security Standard (PA-DSS). This document is also to be used by PA-QSAs as a template to create the Report on Validation.
PCI PTS	PCI PIN Transaction Security Standard This standard includes security requirements for vendors (PTS POI Requirements), device-validation requirements for laboratories (Derived Test Requirements), and a device approval framework that produces a list of approved PTS POI devices (against the PCI PTS POI Security Requirements) that can be referred to by brands' mandates. The PCI PTS list is broken down into the following Approval Classes of devices: PIN Entry Devices (PEDs—standalone terminals), EPPs (generally to be integrated into ATMs and self-service POS devices), Unattended Payment Terminals (UPT), Secure Card Readers (SCRs), and Non-PIN-enabled (Non-PED) POS Terminals.
PCI SSC	The Payment Card Industry Security Standards Council, the organization set up by international payment brands to provide global security requirements applicable to electronic card payment systems. The role of PCI SSC also includes the setting up of standards for the validation of merchants, service providers, and devices against the requirements agreed by brands in PCI SSC. The brands may use approvals issued by PCI SSC in their mandates' requirements.
Sensitive data	PIN, account data, secret keys, and other sensitive keying material that a given device relies on to protect characteristics governed by PCI PTS POI Security Requirements, PCI DSS, and PCI PA-DSS.

2.4 Objectives

This document identifies security guidelines for ATMs, considering the protection that can be provided by the hardware and the software of the ATM itself against attacks aimed at compromising sensitive data acquired, stored, exported, or in any way processed by the device. The primary focus is the mitigation of magnetic-stripe or equivalent image data-skimming and PIN-stealing attacks at ATMs or other ATM manipulation to steal cardholder information, which are most prevalent during the ongoing transition of payment systems to chip technology.

This document is aligned with the security approach and modularity of the PCI PTS POI set of security requirements and is intended to provide:

- Security guidance to acquirers and ATM operators that purchase, deploy, and/or operate ATMs.
- Security guidance and best practices to the ATM industry stakeholders, which includes ATM acquirers, manufacturers, software developers, security providers, refurbishers, et al.

The security guidelines in this document build upon a series of existing standards (IT, security, payment card, and ATM industry). As compromise-prevention best practices, **they are NOT intended to:**

- Provide a set of security requirements for the formal security certification of ATMs.
- Be used as fraud-prevention guidelines (transaction monitoring, card-authentication procedures, etc.)
- Identify guidelines preventing the physical access to the cash stored in the ATM or to the site where the ATM is deployed.
- Identify guidelines for the placement of ATMs.

2.5 Content Organization

Chapter or Annex	Content	
Chapter 3 – Introduction to ATM Security	▪ ATM Services Overview ▪ ATM Security Overview ▪ ATM Technical Standards	
Chapter 4 – ATM Guidelines	**Security Targets**	**Intended Audience**
A – Integration of hardware components	▪ EPP, readers, cabinet, anti-skimming devices ▪ Guidelines for further integrators and software developers	ATM manufacturers, repairing organizations, refurbishers
B – Security of basic software	▪ OS ▪ Middleware (XFS, multivendor software, Open Protocols)	Software integrators, application developers, ATM manufacturers
C – Device management/ operation	▪ Cryptographic/key management, from initialization/distribution to decommissioning ▪ ATM individual security configuration (HW and software) ▪ Environment security	ATM deployers/operators and supporting organizations/service providers
D – Application management	Security functions driven by the ATM application and application management	Application developers, software integrators, ATM operators
Annex 1: ATM Reference Model	A diagram with a generic ATM architecture, its components, and basic interactions	
Annex 2: Criteria for the Privacy Screen Design	An introduction to privacy screen design	
Annex 3: Attack Potential Formula (Adopted from JIL)	An introduction to attack potential calculation ATM individual security configuration (hardware and software)	

3 Introduction to ATM Security

3.1 Background Information

Since the introduction of ATMs in the late sixties in the UK, these card-acceptance devices have been playing a key role both in the bank-services-automation arena and in the 24/7 cash supply to the economy in general as well as to commerce.

ATMs deliver service in a wide range of environments, from bank branches and convenience stores to unattended locations at shopping malls and business centers.

The number of ATMs worldwide reached 2.25 million units by the end of 2010. This number represents growth of 7.3% in one year. Around 100,000 new units were deployed in Asia-Pacific markets alone[1].

Whereas ATMs are primarily engineered to securely store/dispense bank notes and take deposits, they are the preferred self-service platform for an increasing number of services available to cardholders. These include payment of utility bills, topping up of mobile phones, reloading prepaid cards, etc. Other services such as payment of government benefits, entitlements, or micro loans require the disbursement of cash.

As cards and the acceptance infrastructure migrate to chip and NFC technologies, ATMs will continue to play a key role in providing increasingly complex services to chip cards and NFC enabled device holders.

3.2 ATM Security Overview

The cash in transit or stored in the ATM safe has been the asset traditionally targeted by ATM criminals, sometimes in rather violent ways. However, in the last years, attackers have turned their attention equally to soft assets present in the ATM, such as PINs and account data.

Criminals use this stolen information to produce counterfeit cards to be used for fraudulent transactions—increasingly around the world—encompassing ATM withdrawals, purchases with PIN at the point of sale, and purchases without PIN in card-not-present environments.

PINs and account data are assets belonging to cardholders and issuers. They are inevitably in "clear" form at the ATM, when the card and PIN are entered. By attaching, for example, a pinhole camera and a skimmer to the ATM, a criminal can steal PINs and account data before they can be securely processed by the ATM.

These attacks require a relative low attack potential, in terms of both skills and material that is commercially available. The latest generations of skimmers and cameras are unnoticeable to untrained eyes and can be quickly installed and removed from the ATM without leaving any trace. In high traffic ATMs, dozens of PINs and associated account data sets can be stolen in a few hours.

[1] *RBR London,* "Global ATM Market and Forecasts to 2016"

The first line of defense to these attacks has to be offered by the ATM itself. Countermeasures at device level include detection of attached alien objects, disturbance of magnetic-stripe reading near the entry slot, etc. Alarms generated by the device should be acted upon promptly and complemented with inspections of the ATM, more frequently at higher-risk installations.

More sophisticated attacks can involve criminals' locally accessing resources of the PC—USB ports, for example—to install malware and harvest stolen data. These attacks can be combined with or replace remote attacks that exploit vulnerabilities related to the exposure to open networks.

Attackers take advantage of the inherent design and integration of the ATM as a self-service, card-accepting device. The most significant aspects of an ATM's architecture and usage that draw the attention of criminals are as follows:

1. ATM transactions generally require PIN entry and the reading of the card's magnetic stripe and/or the EMV chip. Attackers have therefore the opportunity to capture pairs of PIN and account data that are highly valued in the underground compromised-account-data market.
2. ATMs are generally identified as financial-service-managed devices. They thus generate a level of trust among cardholders that is contradictory to the caution that should be taken when using public-access devices. Cardholders frequently do not exercise the due discretion during PIN entry or do not react to signs of modification of the fascia, etc.
3. For comfort of the cardholder and effective user interface, ATMs offer a large surface to the public. Skimmers or cameras can be hidden or otherwise disguised. Furthermore, holes can be drilled to access the inside of the cabinet.
4. ATMs are also frequently deployed in unattended locations where the likelihood of frequent inspections to detect attachments or tampering is low.
5. ATMs are made of a set of interconnected modules (PC, cabinet, card reader, EPP, etc.) that exchange data through simple protocols and where all modules may not be authenticated or use data encryption. Exchanged data can be tapped into and the underlying data-exchange protocols can be abused if poorly implemented.
6. The PC itself (its OS or network services) can be abused locally and remotely often aided by publicly available information. Malware can be installed or the attacker can access sensitive resources of the PC.

3.3 ATM Technical Standards

Many technical IT security standards have been produced pertaining to ATMs. They address their operation, cryptographic key management, wireless connectivity, operating system hardening, physical security, skimming, etc. They also address different stages of the ATM security life, from configuration to deployment and initialization.

These standards and guidelines are originated at ISO, ANSI, PCI SSC, EPC, and ATMIA or issued by vendors themselves. The most relevant implementation and usage guidelines are listed in the references in this document.

As organized global crime syndicates target ATMs, the financial industry needs a global ATM security standard to promote the availability of secure ATMs. The main characteristics of this standard are:

- Focus on mitigating the effects of skimming and PIN-stealing attacks
- Primarily targeted at products from ATM vendors and deployers
- Provide a complementary framework for device approval (evaluation methodology, evaluation facilities, and approval management)

The current versions of *PCI PTS POI Security Requirements* and *PCI PIN Security Requirements* are excellent starting points for these needed standards. However they are currently defined for POS terminals and their adjustment to ATMs is currently under consideration at the PCI SCC.

Until there is an effective PCI ATM standard, this document fills the perceived current guidance gaps:

- ATM vendors need direction to develop the next generation of ATMs.
- PCI Payment Brand acquirers need support for their procurement processes and to educate their deployers and customers.

4 ATM Guidelines

4.1 Integration of Hardware Components

Objective: **Avert magnetic-stripe and other account data compromise and PIN stealing**

Security targets:
- EPP, readers, cabinet, privacy shields, anti-skimming devices
- The ATM cabinet and the ATM controller
- Guidelines for further integrators and software developers

Intended audience: ATM manufacturers/deployers/operators, ATM integrators, repairing organizations, refurbishers

4.1.1 Security Objectives

Objective	Description	Remarks
A1	Avert physical local attacks that target account data.	Attacks to card readers that include the placement of skimming bugs, with or without the intrusion of the cabinet.
A2	Avert physical local attacks that target PINs.	Attacks include pinhole cameras or other cameras leveraging the ATM surroundings, visual capture, or PIN-pad overlays with manipulation of the cabinet.
A3	Avert attacks aimed at stealing cryptographic, sensitive data stored in secure components.	Examples of secure components include EPPs, card readers (CRs), and extra readers (for example, NFC).
A4	Avert attacks to disable security countermeasures added to the ATM.	Mechanisms like privacy shields and anti-skimming add-ons.
A5	Mitigate potential negative impact stemming from the integration of service modules into ATMs.	Integration of deposit modules, NFC reading pads, etc.
A6	Protect against unauthorized access to sensitive areas and resources in the cabinet, including the fascia.	By service/maintenance staff or attackers.
A7	Produce a security configuration of the ATM model.	Should include: ▪ Hardware components and options ▪ Software components and security parameterization
A8	Provide security guidelines for hardware and software integrators.	To ensure that the subsequent integrators use effective security functions provided by prior integration levels.

Objective	Description	Remarks
A9	Provide security guidelines for service staff.	To first level and second level of maintenance (including staff in charge of routine visual checks)
A10	Ensure that removal or unauthorized access to the EPP triggers an alarm.	EPP is a mandatory security component, and its removal indicates potential attack to PIN.
A11	Prevent modifications of the hardware that may reduce the security protection level.	The inclusion of additional features or modules to the ATM may offer a new attack path. These include poorly designed/installed privacy shields, EPPs, or additional readers. All such modifications should be evaluated and documented to determine if the modification will impact security
A12	Secure the communications between modules within the ATM.	i. In addition to within ATM components, cardholder account data should be protected logically and/or physically when traversing between ATM components. ii. The communication interface(s) of the ATM should not accept connection requests from unauthorized sources.
A13	Contactless data should be secured to 16 points from the point of digitization of the data.	Minimum attack potential of 16 (minimums of 8 for identification and 8 for exploitation) points per ATM, as defined in Annex 3. The point of digitization occurs when the data is processed by the NFC controller and not at the point of entry. The NFC controller acts as a modem, converting the analog signal to a digital signal just as a magnetic-stripe reader or smart-card reader reads data and converts that to a digital signal. In all cases, the point of digitation is where the wireless signal is converted to a digital data stream.

4.1.2 Guidelines and Best Practices

Guideline/Best Practice	Remarks
a) The EPP should have a valid PCI PTS POI approval.	i. The EPP model should have the security approval listed in the PCI SSC web site
b) If the ATM permits access to internal areas that process or store account data (e.g., for service or maintenance), it is not possible using this access area to insert a bug that would disclose any sensitive data.	i. Encryption of account data between security-relevant components or sufficiently strong walls, doors, and mechanical locks may be sufficient to meet this guideline. ii. Minimum attack potential of 16 (minimums of 8 for identification and 8 for exploitation) points per ATM, as defined in Annex 3. .
c) The hardware and any changes to it thereafter have been inspected and reviewed using a documented and repeatable process, and certified as being free from hidden and unauthorized or undocumented functions.	i. It is essential to list the security options in an ATM model to be able to assess the overall security level and the impact of changes in security protection levels when ATM modules are introduced or removed (NFC reader, deposit module, etc.).
d) Hardware development and integration should be subject to a well-structured process including formal specification, test plans, and documentation. Hardware is released only if tests according to the test plan were successful.	i. The integration of SCRs or EPPs compliant to the applicable PCI PTS POI Security Requirements may facilitate the ATM following this guideline.
e) The integration of the EPP and any mechanisms protecting against unauthorized removal are properly implemented and follow the guidelines provided by the device vendor.	i. Minimum attack potential of 18 (minimums of 9 for identification and 9 for exploitation) points per ATM, as defined in Annex 3. ii. The integration guidance is validated during the EPP's PTS evaluation and approval.
f) The fascia and cabinet design or the mechanical integration of the EPP should not facilitate the visual observation of PIN values as the cardholder is entering them.	i. A privacy screen and other visual observation deterrents (such as placement of the EPP combined with defensive posture of the cardholder's body) should facilitate the ATM following this guideline.
g) The ATM is equipped with mechanisms or otherwise designed to prevent or deter the attacks aiming at retaining the payment card (and recovery by the attackers when cardholder leaves the ATM).	i. For example, card trapping, Lebanese Loop attack.

Guideline/Best Practice	Remarks
h) The ATM is equipped with mechanisms to prevent or deter attempts to modify or penetrate the ATM to make any additions, substitutions, or modifications to the magnetic-stripe reader or the ATM's hardware or software, in order to determine or modify magnetic-stripe track data.	i. The compliance of the reader to Evaluation Module 4 (SRED) of the *PCI PTS POI Security Requirements* may greatly facilitate the ability of the ATM to follow this guideline. ii. The installation, where feasible, of two card readers (CRs) with segregated reading technologies (chip and magnetic-stripe) may greatly contribute to following this guideline iii. Minimum attack potential of 16 (minimums of 8 for identification and 8 for exploitation) points per ATM, as defined in Annex 3.
i) The integration of secure card readers, SCRs and, if applicable, any mechanisms protecting against SCR's unauthorized removal, are properly implemented and follow the guidelines provided by the embedded device vendor.	i. SCRs are readers approved under the PCI PTS SCR Approval Class.
j) The logical and physical integration of CRs into the ATM does not create new attack paths to account data.	

Guideline/Best Practice	Remarks
k) The ATM should be equipped with mechanisms preventing skimming attacks against account data: ○ There should be no demonstrable way to disable or defeat the mechanisms and installing an external or internal skimming device to a minimum attack potential. ○ If not equipped with anti-skimming mechanisms or with mechanisms that do not reach the minimum attack potential, there should be manual control procedures in place so that the ATM is periodically inspected for the presence of skimming devices. The inspections should include remote and/or local procedures; their frequency should be a function of the risk of the installation and they should be triggered when alarms indicate potential attachment of a skimming device. ○ Detection by an anti-skimming device of a skimming attack or any tampering attempt should result in the closure of the machine or the issuance of an alert. ○ Changes in the environment of the card slot should always be detected after ATM is powered on.	i. Minimum attack potential of 16 (minimums of 8 for identification and 8 for exploitation) points per ATM for the anti-skimming mechanisms, as defined in Annex 3. ii. An ATM should be equipped with an anti-skimming device according to at least one of the following anti-skimming methods: ○ The device is able to prevent attachment or placement inside a card reader of a skimming device or a partly or completely fake ATM front on a card-reader. Such an anti-skimming device should be equipped with active removal and modification detection functionality to shut down the ATM when activated. ○ The device is able to detect attachment of a skimming device or a partly or complete fake ATM front on a card-reader. Such an anti-skimming device should be equipped with a detection functionality to shut down the ATM when activated, ○ The device is able to disturb the reading of the magnetic stripe by attached devices whenever a card is entered into the card reader. ○ The device is able to detect or prevent the placement of a skimming device in-between the fascia and the reader (e.g., with internal/motorized readers).

Guideline/Best Practice	Remarks
k) *continued*	iii. The ATM monitoring system should be able to remotely detect whether electronic anti-skimming solutions are operational. iv. When a card is inserted into the card slot and the card transport does not function accordingly, the ATM should stop operating and return the card. When an ATM is closed for operation it should not be possible to enter the PIN, and a corresponding warning should be displayed. v. If the card-reader entrance opening has a recess to grasp the card, the shape of this recess should make it difficult to install an external device to capture magnetic-track data or the card slot should be designed with a clean and smooth fascia such that any foreign additions can be more easily detected. vi. The materials used to build the card-entrance area should have anti-vandal characteristics in order to make its removal or destruction tamper evident. vii. Security cameras may be used to detect the attachment to the fascia of external skimmers.
l) The ATM should be equipped with only one cardholder PIN-acceptance interface, the ATM PCI PTS-approved EPP.	i. Only the EPP can be used for PIN entry.
m) If the EPP can be used for non-PIN data entry, the unauthorized alteration of prompts for non-PIN data entry into the EPP cannot occur without requiring a minimum attack potential.	i. PINs may be compromised when malware prompts for the PIN entry when the EPP output is not encrypted. ii. Minimum attack potential of 16 (minimums of 8 for identification and 8 for exploitation) points per ATM, as defined in Annex 3.

Guideline/Best Practice	Remarks
n) If the ATM supports any input devices other than the EPP, including touch screens, both the ATM display and additional input devices should be securely protected so that it is not possible to alter display prompts or log key entry without requiring a minimum attack potential.	i. Minimum attack potential of 18 (minimums of 9 for identification and 9 for exploitation) points per ATM, as defined in Annex 3. ii. Any input device should be securely controlled so that it is not possible to maliciously abuse it to capture PINs. iii. All user interfaces—e.g., HTML, scripts, etc.—should be protected against manipulation at all times.
o) Where possible and allowed by law, the ATM should be equipped with a security camera.	i. The location for camera installation should be carefully chosen to ensure that images of keypad entry are not recorded. ii. The camera should support the detection of the attachment of alien devices to the fascia and possess the ability to generate an alarm for remote monitoring if the camera is blocked or otherwise disabled.
p) The integration of the EPP into the ATM fascia should be engineered in a way that the ATM does not facilitate the fraudulent placement of an overlay over the PIN pad.	i. Features like recesses in the fascia, bezels, or a privacy shield may facilitate or disguise the attachment of a thin, fraudulent keypad over the EPP keypad.

4.2 Security of Basic Software

Objective: Avert magnetic-stripe skimming and PIN stealing

Security targets:
- Operating System, BIOS
- Middleware (XFS, CEN XFS, CEN J/XFS, multivendor software, Open Protocols)

Intended audience: Software integrators, application developers, ATM manufacturers/deployers/operators

4.2.1 Security Objectives

Objective	Description	Remarks
B1	Prevent abuse of OS and reduce the attack surface of the ATM OS platform (Windows) and BIOS.	▪ Operating system should be hardened or parameterized so as to prevent abuse of privileges, default accounts, installation of malicious software, and unauthorized access to resources like USB ports/CDs/DVDs/hard disks. ▪ The OS should enforce strict application separation, for example prevent the unauthorized usage of the various services (OS, Platform, including XFS and Applications) should be prevented at all times e.g., runtime, service and administration. ▪ It should not be possible to install rogue software. (Both with and without physical access should be considered.) ▪ Hardening/locking-down guidelines issued by the OS supplier should be strictly followed.
B2	Prevent exploitation of public domain vulnerabilities in the Open Protocols stack.	Ensure the regular security review and the patching of minimum set of protocols used.
B3	Reduce attack surface from public and private networks.	The communication interface should be hardened.
B4	Prevent abuse by software suppliers.	Software from third-party middleware vendors (for example, multivendor ATM application emulators) and other software should be tested before installation or usage. For example, PA-DSS requirements should be applied to banking applications to facilitate the protection of account and PIN data.

Objective	Description	Remarks
B5	Use effective network isolation and intrusion detection/mitigation tools.	Network isolation and intrusion detection/mitigation tools should be used.
B6	Trace/log OS activity.	OS should be parameterized to log all relevant events.
B7	Protect sensitive functions and enforcement mechanisms for appropriate key-loading procedures.	▪ Example of sensitive functions: firmware loading, loading of clear, initial keys. ▪ Access to the AC should require administrator rights.
B8	Protect against unauthorized changes.	To ensure protection against malware.
B9	Protect against the unauthorized remote control of the application.	Strict access-control procedures should be put in place to allow remote access for service purposes.
B10	Protect again unauthorized installation of software.	ATMs have a multi-layer software stack consisting of: 1) The operating system, 2) The platform together with the respective hardware drivers and support for CEN XFS - CEN J/XFS, and 3) The software application.

4.2.2 Guidelines and Best Practices

Guideline/Best Practice	Remarks
a) The ATM performs a self-test upon start-up and at least once per day to check the software of the AC, the security mechanisms under the control of the ATM for signs of tampering, and whether the ATM is in a compromised state. In the event of a failure, the ATM and its functionality should fail in a secure manner.	i. Core software mechanisms exist to validate banking applications.
b) The ATM uses and relies upon the EPP functions and control mechanisms for key loading and key management, as evaluated during the PCI PTS EPP approval process.	i. An example of a sensitive EPP function is the loading of clear initial keys under the principles of dual control and split knowledge.

Guideline/Best Practice	Remarks
c) Access to sensitive services requires authentication. Sensitive services provide access to the underlying sensitive functions. Entering or exiting sensitive services should not reveal or otherwise affect sensitive information.	i. Examples of sensitive functions supported are: ○ Administrator access to the AC ○ ATM software updates ○ Physical access, for the purpose of maintenance, to locations where account data is processed
d) To minimize the risks from unauthorized use of sensitive services, limits on time and the number of actions that can be performed should be imposed, such as session time outs for operator inactivity, after which the ATM is forced to return to its normal mode.	
e) If the ATM supports multiple applications, it should enforce the separation between the applications. It should not be possible that one application interferes or tampers with another application or the OS of the ATM, including its ability to access, use, or modify data objects belonging to another application—even if they are distributed over separate components of the ATM.	i. Applications are considered to be separated by access rights. OS is considered all code that is responsible to enforce, manage, or change such access rights. ii. Focal point is for sensitive data and sensitive functions. This includes keys stored in the EPP and card readers and is in scope for applications executing in the AC or remotely.
f) The ATM should implement provisions against unauthorized modification of the software configuration, including the operating system, drivers, libraries, and applications.	i. Minimum attack potential of 18 (minimums of 9 for identification and 9 for exploitation) points, as defined in Annex 3. ii. The software configuration includes the platform software, platform configuration data, applications loaded to and executed by the platform, and its data. The mechanisms should also allow ensuring the integrity of third-party applications, using an authorized process to install it.

Guideline/Best Practice	Remarks
g) The operating system and the software of the ATM should contain only the components and provide only the services exclusively needed for the operation or those that are protected under defined security policies. The OS should be configured and run with least privilege.	i. OS modules such as peripheral drivers, file systems, or inter-process communication protocols should be regarded as components. Applications responding to external interfaces should be regarded as services. ii. All unused applications should be removed (e.g., games, administrative utilities). iii. All unused background services (e.g. print spooler, DHCP client) should be disabled.
h) The access-control mechanisms of the ATM should support a distinction between persons and roles that are needed to administer and operate the ATM.	i. This guideline may be followed by properly using OS security policies. ii. The list of roles should at least consist of: ○ Normal ATM operations like loading/unloading money, paper, and retracted cards ○ Technical maintenance ○ Software configuration ○ Key management ○ Auditing
i) The ATM platform should implement reliable logging for the purpose of security. The logging should include at least: ○ Activation of the service interface(s); ○ All maintenance operations; and ○ Physical access to the inside of the ATMs.	i. This guideline may be met with proper implementation of OS security policies. ii. The logging of regular transactions should be included. iii. The logging can occur at host level.
j) The logging data should be stored in a way that the data cannot be changed or deleted without proper authorization.	
k) Access to the service interface(s) requires identification and authentication. Any remote service interface should be protected against information disclosure and intrusion.	i. While service functions are performed, the ATM should not perform cardholder transactions. ii. Strong cabinet walls and proper locks may facilitate this practice.

Guideline/Best Practice	Remarks
l) The communication interface(s) of the ATM should be protected against intrusion and misuse from outside. The ATM should implement dedicated countermeasures (OS should be hardened) and keep up-to-date with patches.	i. Should be compliant to Evaluation Module 3: Open Protocols of the *PCI PTS POI Security Requirements*. ii. The communication interface(s) of the ATM should not accept connection requests from unauthorized sources.

4.3 Device Management/Operation

Objective: Ensure adequate management of:

- ATM during manufacturing
- ATM in storage of deployed ATM estates
- ATM individual security configuration (hardware and software)

Security targets:

- Cryptographic/key management, from initialization/distribution to decommissioning
- Manufacturing management system
- Estate management process and tools
- Environmental security

Intended audience: ATM manufacturers/deployers/operators and supporting organizations/service providers

4.3.1 Security Objectives

Objective	Description	Remarks
C1	Put in place adequate controls for the device's production, transportation, storage, and use throughout its life cycle until initial deployment.	
C2	Ensure adequate cryptographic initialization and service.	
C3	Ensure secure distribution of software, updates/patches that impact security, and non-financial applications, including advertisements.	
C4	Manage an updated inventory of ATMs and their configurations, including their hardware, software, logs and reports.	
C5	Manage the life cycle, from manufacturing and initialization through decommissioning.	
C6	Specify and execute proper security decommissioning procedures.	
C7	Ensure the spare parts and decommissioned ATMs or parts have keying information and other sensitive data removed.	
C8	Support user education at the ATM.	

4.3.2 Guidelines and Best Practices

Guideline/Best Practice	Remarks
a) Change-control procedures are in place so that any intended change to the physical or logical capabilities of security-relevant components of the ATM are identified and appropriate measures are taken.	
b) The software is protected and stored in such a manner as to preclude unauthorized modification—e.g., using dual control or standardized cryptographic authentication procedures.	i. Loading of software into the ATM should be performed by the ATM deployer, by the manufacturer, or by a third party acting on behalf of the acquirer.
c) The ATM is assembled in a manner to ensure that the components that handle/process cardholder data and are used in the manufacturing process are those components that were certified, and that unauthorized substitutions have not been made.	
d) Production software that is loaded to devices at the time of manufacture or deployment is transported, stored, and used under the principle of dual control, preventing unauthorized modifications and/or substitutions.	
e) Subsequent to production but prior to shipment from the manufacturer's facility, the ATM and any of its components are stored in a protected, access-controlled area or sealed within tamper-evident packaging to prevent undetected unauthorized access to the device or its components.	
f) If the ATM's security-relevant components will be authenticated at the facility of initial deployment by means of secret information placed in the device during manufacturing, then this secret information is: ○ Unique to each ATM, ○ Unknown and unpredictable to any person, and ○ Installed in the ATM under dual control and split knowledge to ensure that it is not disclosed during installation.	

Guideline/Best Practice	Remarks
g) Security measures are taken during the development and maintenance of ATM security-related components. The manufacturer should maintain development-security documentation describing all the physical, procedural, personnel, and other security measures that are necessary to protect the integrity of the design and implementation of the ATM security-related components in their development environment. The development-security documentation should provide evidence that these security measures are followed during the development and maintenance of the ATM security-related components. The evidence should justify that the security measures provide the necessary level of protection to maintain the integrity of the ATM security-related components.	
h) Controls exist over the repair process and the inspection/testing process subsequent to repair to ensure that the device has not been subject to unauthorized modification.	
i) The ATM security-relevant components should be protected from unauthorized modification with tamper-evident security features, and customers should be provided with documentation (both shipped with the product and available securely online) that provides instruction on validating the authenticity and integrity of the ATM.	
j) Where this is not possible, the ATM is shipped from the manufacturer's facility to the facility of initial deployment and stored en route under auditable controls that can account for the location of every ATM at every point in time.	
k) Where multiple parties are involved in organizing the shipping, it is the responsibility of each party to ensure that the shipping and storage that they are managing is compliant with this requirement.	

Guideline/Best Practice	Remarks
l) Procedures are in place to transfer accountability for the device from the manufacturer to the facility of initial deployment. Where the device is shipped via intermediaries such as resellers, accountability will be with the intermediary from the time at which they receive the device until the time it is received by the next intermediary or the point of initial deployment.	
m) While in transit from the manufacturer's facility to the facility of initial deployment, the device's security-relevant components are: ○ Shipped and stored in tamper-evident packaging; and/or ○ Shipped and stored containing a secret that: – Is immediately and automatically erased if any physical or functional alteration to the device is attempted, and – Can be verified by the initial-key-loading facility but cannot feasibly be determined by unauthorized personnel.	
n) The device's development-security documentation should provide means to the facility of initial deployment to assure the authenticity of the target of evaluation's security-relevant components.	
o) If the manufacturer is in charge of initial-key loading, the manufacturer should verify the authenticity of the ATM security-related components.	
p) If the manufacturer is not in charge of initial-key loading, the manufacturer should provide the means to the facility of initial deployment to assure the verification of the authenticity of the ATM security-related components.	
q) Each security-relevant device should have a unique, visible identifier affixed to it or should be identifiable using secure, cryptographically protected methods.	

Guideline/Best Practice	Remarks
r) The vendor should maintain a manual that provides instructions for the operational management of the ATM. This includes instructions for recording the entire life cycle of the ATM security-related components and of the manner in which those components are integrated into a single ATM, e.g.: ○ Data on production and personalization ○ Physical/chronological whereabouts ○ Repair and maintenance ○ Removal from operation ○ Loss or theft	
s) Upon decommissioning of an ATM, all sensitive information and sensitive technical parts should be removed or destroyed.	i. All encryption keys, security parameters, ATM software and branding stickers should be removed. ii. Lock/locking mechanisms and electronic security systems should be removed or destroyed to avoid that they can be analyzed for illegal purposes as for example attack preparation. iii. Make sure that all data storage and processors including security processors are zeroized.
t) Store decommissioned ATMs in a particular storage area assigned for the purpose.	i. The storage area should be under appropriate supervision and should be equipped with appropriate locks and alarms. ii. Each ATM in storage should be registered in an inventory list that is checked regularly.
u) On ATM or vicinity, display warnings to customers: ○ To “protect and shield their PINs” ○ Informing about skimming devices, along with details of a customer helpline to report incidents	i. General advice on ATM security to be published for customer education. ii. ATM screens can be used to display how the unaltered ATM and card reader should appear.

Guideline/Best Practice	Remarks
v) Procedural or automated controls should exist to prevent the capture of cardholder account data in card readers used to access the area housing the ATMs.	i. Facades for vestibule access doors that require the cardholder to swipe their card in order to gain entry to the enclosed area housing the ATMs can be used to hold skimming devices, and preventive and/or detective mechanisms should exist to prevent the capture of cardholder account data.

4.4 ATM Application Management

Objective: Address security aspects of the ATM application.

Security targets: Security functions driven by the ATM application and application management

Intended audience: Application developers, software integrators, ATM operators

4.4.1 Security Objectives

Objective	Description	Remarks
D1	Enforce best practices for application development, testing and distribution.	
D2	Ensure the effectiveness of security functions driven by the application.	Encryption of sensitive data in transit.
D3	Ensure the ATM application interacts securely with the ATM display and EPP.	

4.4.2 Guidelines and Best Practices

Guideline/Best Practice	Remarks
a) The ATM application should enforce the correspondence between the display messages visible to the cardholder, the operating state of the ATM, and the application the cardholder interacts with. It should especially be obvious to the cardholder when the PIN-entry keypad is operated in a clear mode, and when the PIN is being entered, and for which application.	i. The ability to physically access the connection between devices (e.g., EPP, AC, and ICC reader) should not facilitate attacks to interfere with that correspondence and especially to collect clear PIN data (e.g., commands are authenticated and/or enciphered). Keys used for such protocols should only be used for this purpose and may then be stored and used in the AC in the clear. It is not required to use a cryptographic module in the AC for that purpose. ii. Minimum attack potential of 16 (minimums of 8 for identification and 8 for exploitation) points, as defined in Annex 3.

Guideline/Best Practice	Remarks
b) ATM applications that are controlled or executed remotely should use trusted communication channels and be authenticated while they are executed. Cryptographically based controls are to be utilized to control the ATM display and ATM usage such that it is infeasible for an entity not possessing the unlocking mechanism to alter the display and to allow the output of unencrypted PIN data from the ATM.	i. The controls provide for unique accountability and utilize key sizes appropriate for the algorithm(s) in question. Key-management techniques and other control mechanisms are defined and include appropriate application of the principles of dual control and split knowledge.
c) The entry of any other transaction data should be separate from the PIN-entry process, avoiding the accidental display of a cardholder PIN on the ATM's display. If other data and the PIN are entered on the same keypad, the other data entry and the PIN entry should be clearly separate operations.	
d) The transaction data transferred over the communication interface should be protected with adequately strong mechanisms against disclosure. If open channels (like wireless links or an Internet connection) are used, the data should be encrypted.	i. Account data should be protected in accordance with PCI DSS and PCI PA-DSS.
e) Sensitive information should not be present any longer or used more often than strictly necessary. The ATM should automatically clear its internal buffers when either: ○ The transaction is completed, or ○ The ATM has timed out waiting for the response from the cardholder or host.	
f) Prevent the display or disclosure of cardholder account information.	i. Displayed on ATM screen, audio transcript for visually impaired cardholders, or printed on receipts.

5 About the PCI Security Standards Council

The mission of the PCI Security Standards Council is to enhance payment account security by driving education and awareness of the PCI Data Security Standard and other standards that increase payment data security.

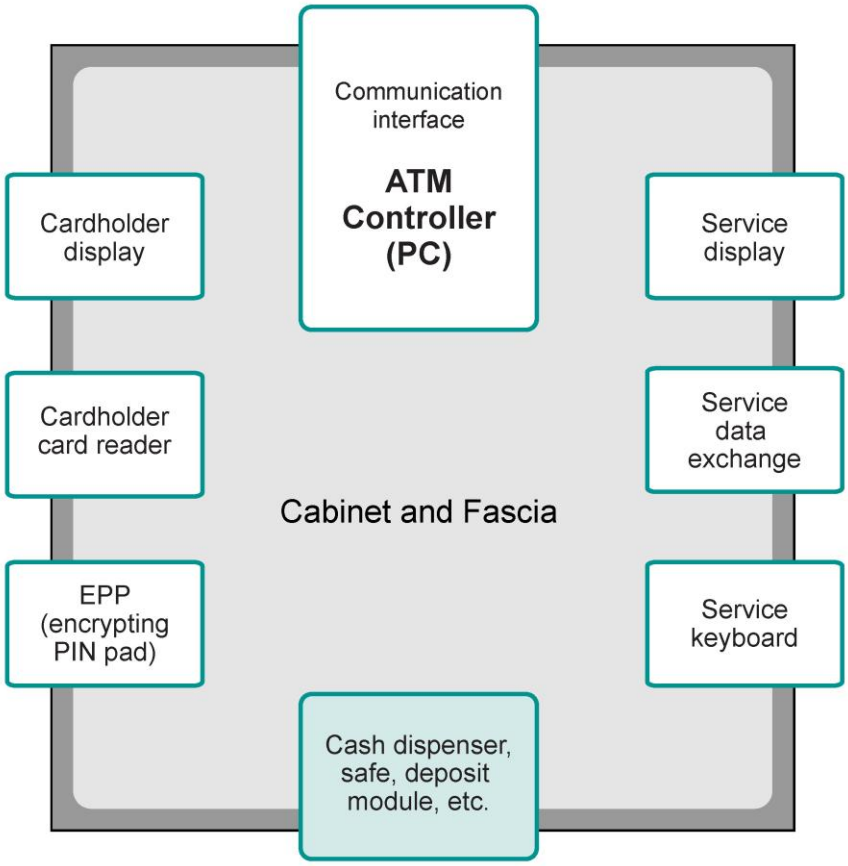
The PCI Security Standards Council was formed by the major payment card brands American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. to provide a transparent forum in which all stakeholders can provide input into the ongoing development, enhancement, and dissemination of the PCI Data Security Standard (DSS), PIN Transaction Security (PTS) Requirements, and the Payment Application Data Security Standard (PA-DSS). Merchants, banks, processors, and point-of-sale vendors are encouraged to join as Participating Organizations.

Annex 1: ATM Reference Model

This annex describes the functional/security building blocks of a typical ATM.

The ATM model considered in these guidelines is depicted below. It addresses ATM components that, under attack, may lead to the compromise of sensitive data (PIN, account data or keys).

Components of the ATM, such as the cash dispenser or the safe, that are not directly related to compromise of PIN or account data, are not within the scope of the ATM model.



The ATM components and design properties of interest to these guidelines are:

- The encrypting PIN pad (EPP) contains an embedded cryptographic module, which exclusively performs the tasks of PIN encryption and key management. The EPP's cryptographic module often provides other cryptographic services, such as message encryption and message authentication.
- The card reader, which can be a hybrid reader or multiple readers, each with a specific technology (chip or magnetic stripe). Readers may or may not be motorized.
- The ATM cardholder display. The display is usually directly connected to the AC (PC) and is assumed as a passive device, which cannot authenticate any other part or decrypt message content.

- The AC, which tends to be a standard PC operated by a standard operating system like Windows XP. The set of software including the operating systems, drivers and libraries (like the XFS), providing the environment for an ATM application, is called the “ATM Platform,” provided by the ATM vendors, whereas a specific “ATM application” is often provided by the ATM operator or deployer.
- The physical properties of the ATM cabinet and fascia, which restrict access to the ATM components. Cabinet design can be important in mitigating the effects of shoulder-surfing, installation of PIN pad overlays, or skimmers.
- The communication interface to the authorization host or other networked resources. In addition, the ATM may be equipped with a service interface composed of:
  - A service keyboard,
  - A service display, and
  - A service data exchange module, which may consist of a card reader, a floppy disk drive, a USB interface, or similar.

  The service-interface components may be partially remote.

Annex 2: Criteria for the Privacy Screen Design

The following are examples of device privacy screens being provided by the device itself that are compliant with *PCI PTS POI Security Requirements*. Other designs may also be acceptable.

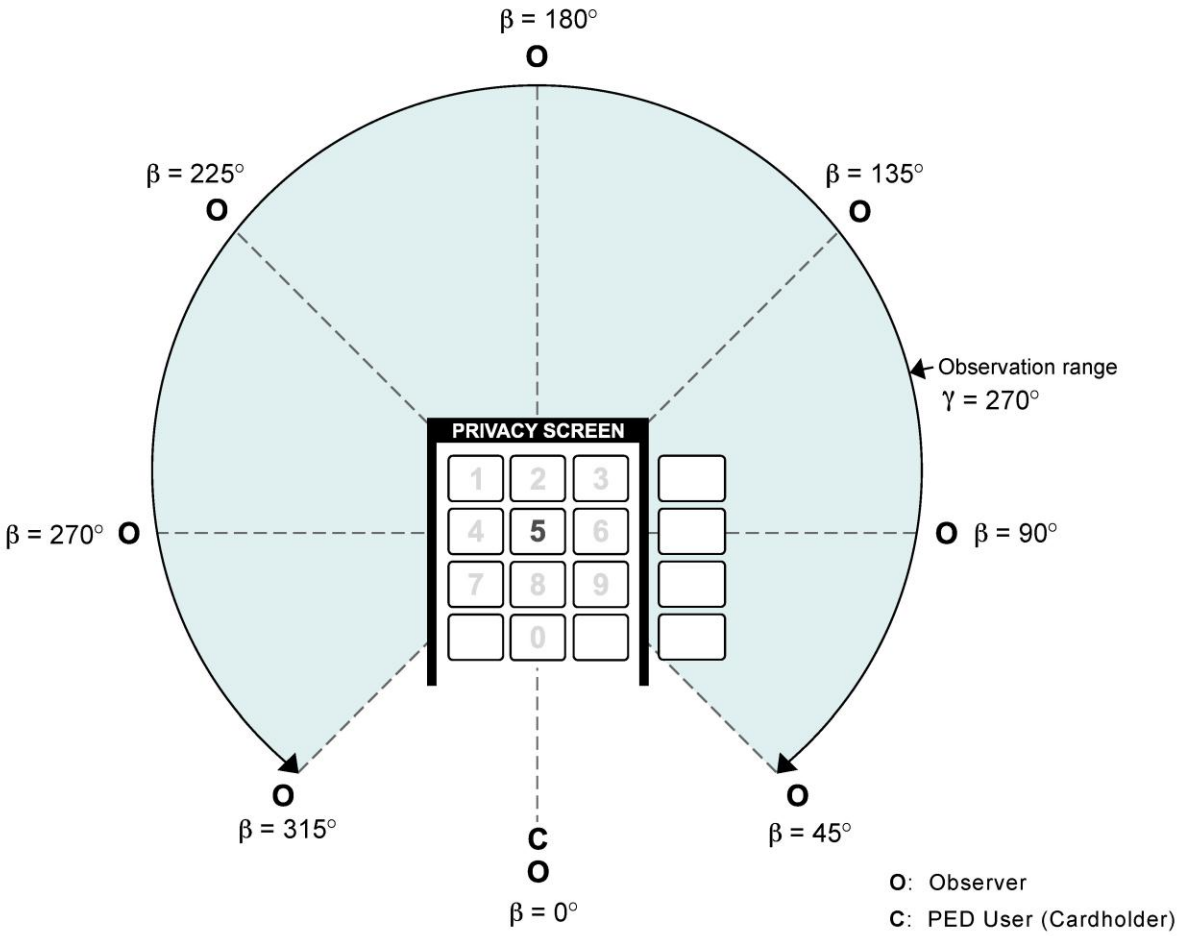


Figure A1: Sample device with privacy screen range, bird's eye view

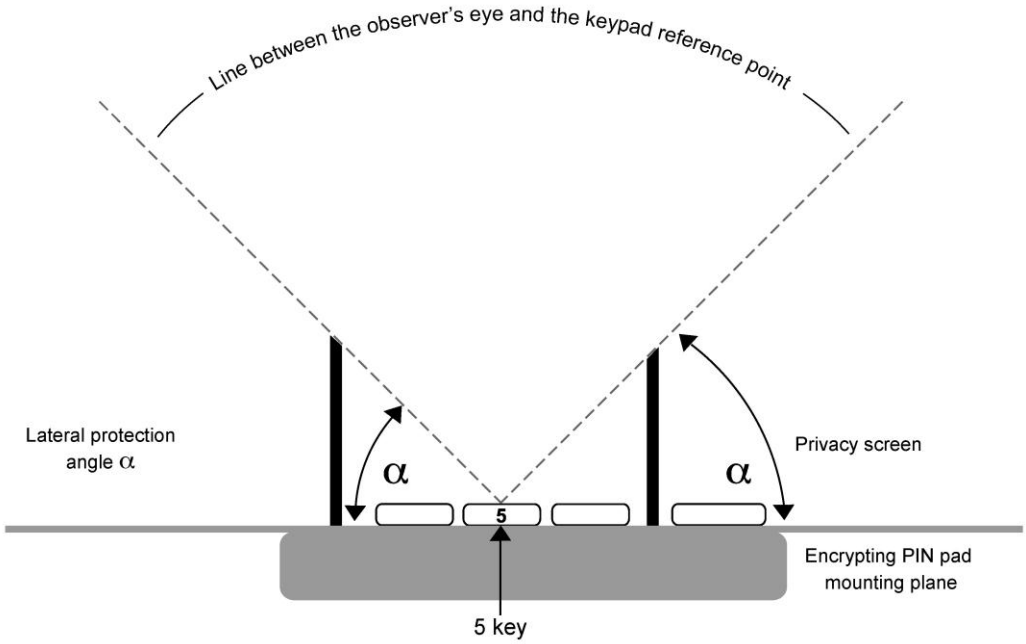


Figure A2: Sample device keypad, sectional drawing from the "0" side

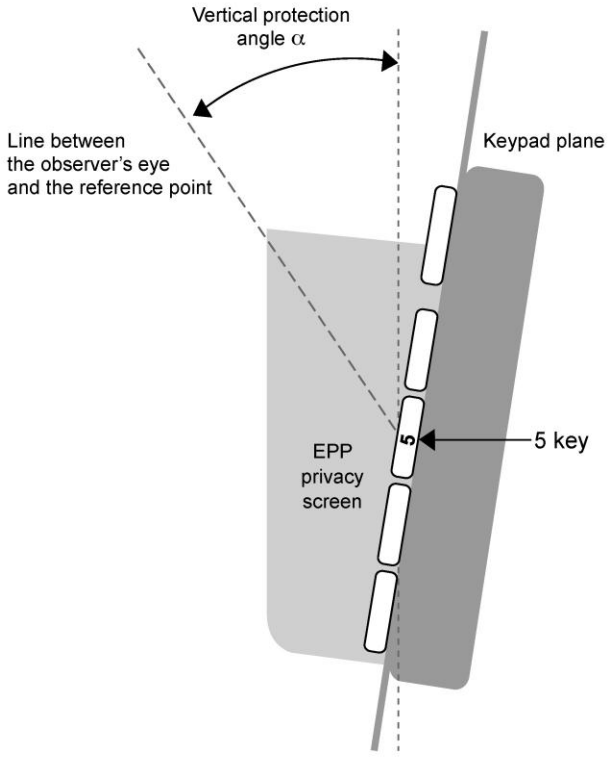


Figure A3: Sample device keypad, side view

The angles in the figures above are defined as follows:

α: Angle between the vertical plane through the '5' key and a virtual line which connects the '5' key and an observer's eye

β: Horizontal position of an observer relative to the PIN entry device's position

γ: Horizontal range which is to be covered by the privacy screen

δ: Angle between the keypad plane and the horizontal plane

Design rules:

1. These definitions apply to a privacy shield, which is provided as design property by the device. It may be a part of the PIN entry device, or provided by the device's cabinet. The rules and the figures above are to be considered as guidelines, which may be replaced by other means of at least the same efficiency.
2. The keypad reference point is taken as the column position in the middle of the keypad in the row containing the numeric key '5.'
3. The privacy screen of the device is to be placed horizontally or slightly tilted ($0 \leq \delta \leq 45°$) and shall provide the following protection angles:

Horizontal angle β	Remark	Vertical angle α
$315° \leq \beta \leq 45°$:	Within this range of β the cardholder deters an observer with her/his body.	N/A
$45° \leq \beta \leq 90°$ $270° \leq \beta \leq 315°$:	Within these ranges visual observation of the keypad is partially blocked by the cardholder. The protection angle α shall be at least 35°. Please note that the front end of the privacy screen must be higher if the device is tilted.	$\alpha \geq 35°$
$90° \leq \beta \leq 270°$:	The protection angle shall be at least 40°. The display side of the privacy screen may be lowered as the device is tilted against the horizontal plane.	$\alpha \geq 40°$

   The vertical angles given in the table above are with respect to the horizontal plane (see figure above). If by design of the device the keypad is tilted toward the cardholder, the backside of the privacy screen may be lower.
4. If the device is to be placed vertically or tilted by 45° or more, the requirements under Step 3 will apply accordingly, using the vertical plane instead of the horizontal plane as the reference for the angle α.
5. The protection is based on viewing angles and does not imply a specific technical implementation like physical shields. If the keypad is implemented as a touch screen, the viewing barrier may be implemented by polarizers (e.g., as film on the touch screen surface), which deter the observation from the sides. The up (clerk) side must be implemented as a physical shield.

Annex 3: Attack Potential Formula (Adopted from JIL)

Introduction to attack potential calculation

Certain guidelines in this document refer to a minimum attack potential in points. These points represent the effort necessary to defeat a given security mechanism using a range of resources (time, skills, prior knowledge, etc.).

Calculating Attack Potentials

This section examines the factors that determine attack potentials and provides some guidelines to help remove some of the subjectivity from this aspect of the evaluation process. This approach should be adopted unless the evaluator determines that it would be inappropriate, in which case a rationale is required to justify the validity of the alternative approach

Identification and Exploitation

For an attacker wanting to exploit vulnerability, the vulnerability must first be identified. This may appear to be a trivial separation, but it is an important one. To illustrate this, first consider a vulnerability that is uncovered following months of analysis by an expert, and a simple attack method published on the Internet. Compare this to a vulnerability that is well known but requires enormous expenditure of time and resources to exploit. Of course, factors such as time need to be treated differently in these cases.

In this document, “exploitation” and “initial exploitation” are alternatively used to designate “initial exploitation.”

Factors to be Considered

The following factors should be considered for the analysis of the attack potentials required to exploit vulnerability:

1. **Identification**
   a) Attack time for the various levels of expertise;
   b) Potential to acquire the required knowledge of the ATM’s design and operation;
   c) Potential for the access to the ATM;
   d) Equipment required like instruments, components, IT hardware, software required for the analysis;
   e) ATM specific spare components
2. **Exploitation**
   a) Attack time for the various levels of expertise;
   b) Potential to acquire the required knowledge of the ATM’s design and operation;
   c) Potential for the access to the ATM;
   d) Equipment required like instruments, components, IT hardware, software required for the analysis;
   e) ATM specific spare components.

In many cases these factors don't depend on each other but might be substituted for each other in varying degrees. For example, expertise or hardware/software can be a substitute for time. A discussion of these factors follows.

The **attack time** is given in the time in hours taken by an attacker to identify or exploit an attack. If the attack consists of several steps, the attack time can be determined and added to achieve a total attack time for each of these steps. Actual labor time has to be used instead of time expired as long as there is not a minimum attack time enforced by the attack method applied (for instance, the time needed for performing a side channel analysis or the time needed for an epoxy to harden). In those cases where attendance is not required during part of the attack time, the attack time is to be taken as expired time divided by 3.

Expertise refers to the level of generic knowledge of the application area or product type (e.g., UNIX operation systems, Internet protocols). Identified levels are as follows:

a) **Experts** are familiar with the underlying algorithms, protocols, hardware, structures, etc. implemented in the product or system type and the principles and concepts of security employed;

b) **Proficient** persons are knowledgeable in that they are familiar with the security behavior of the product. For the purposes of exploitation, proficient persons qualify when specific skills are required to conduct an attack successfully.

c) **Laymen** are unknowledgeable compared to experts or proficient persons, with no particular expertise. For the purpose of exploitation, they can implement an attack based on a script or a written procedure, without requiring any particular skill.

If proficient expertise on various areas of technology is required for an attack, e.g., on electrical engineering and cryptography, an expert level of expertise can be assumed.

Knowledge of the ATM refers to obtaining specific expertise in relation to the ATM. This is different from generic expertise but not unrelated to it. Identified levels are as follows:

a) **Public information** about the ATM (or no information): Information is considered public if it can be easily obtained by anyone (e.g., from the Internet) or if it is provided by the vendor to any customer.

b) **Restricted information** concerning the ATM (e.g., as gained from vendor technical specifications): Information is considered restricted if it is distributed on request and the distribution is registered (e.g., like the *PCI PTS HSM DTRs*).

c) **Sensitive information** about the ATM (e.g., knowledge of internal design, which may have to be obtained by "social engineering" or exhaustive reverse engineering).

Care should be taken here to distinguish between information required to identify the vulnerability and the information required to exploit it, especially in the area of sensitive information. Requiring sensitive information for exploitation would be unusual.

Specialist expertise and **knowledge of the ATM** are concerned with the information required for persons to be able to attack an ATM. There is an implicit relationship between an attacker's expertise and the ability to effectively make use of equipment in an attack. The weaker the attacker's expertise, the lower the potential to effectively use equipment. Likewise, the greater the expertise, the greater the potential for equipment to be used in the attack. Although implicit, this relationship between expertise and the use of equipment does not always apply—for instance, when environmental measures prevent an expert attacker's use of equipment; or when, through the efforts of others, attack tools requiring little expertise for effective use are created and freely distributed (e.g., via the Internet).

Access to the ATM is also an important factor. It is assumed here that the ATM would be purchased or otherwise obtained by the attacker and that beside other factors there is no time limit in analyzing or modifying the ATM. Differences are defined in the status and functionality of the device to be analyzed/tested.

a) **Mechanical samples** are non-functional and are used merely to study the mechanical design or for supplying spare parts.

b) **Functional samples without working keys** might be used for the logical and electrical behavior of the device but are not loaded with working keys and are therefore not functional within a payment network or with real payment cards. Such devices might be regularly purchased. Please note that these also include devices fitted with test or dummy keys.

c) **Functional samples with working keys** are fully functional devices, which might be used to verify an attack method or to actually perform an attack.

If more than one sample is needed in any category, instead of multiplying the points by the number of samples, the following factors must be used:

Table 1: Multiple Samples Factors

Number of Devices	Factor
1	1
2-4	1.5
>5	2

In the case that more than one sample is accounted for, strong justification must be provided for the use of multiple samples.

Equipment refers to the equipment that is required to identify or exploit vulnerability.

a) **Standard equipment** is equipment that is readily available to the attacker, either for the identification of vulnerability or for an attack. This equipment can be readily obtained—e.g., at a nearby store or downloaded from the Internet. The equipment might consist of simple attack scripts, personal computers, card readers, pattern generators, simple optical microscopes, power supplies, or simple mechanical tools.

b) **Specialized equipment** isn't readily available to the attacker, but could be acquired without undue effort. This could include purchase of moderate amounts of equipment (e.g., dedicated electronic cards, specialized test bench, protocol analyzers, oscilloscopes, microprobe workstation, chemical workbench, precise milling machines, etc.) or development of more extensive attack scripts or programs.

c) **Bespoke equipment** is not readily available to the public, as it might need to be specially produced (e.g., very sophisticated software), or because the equipment is so specialized that its distribution is controlled, possibly even restricted. Bespoke equipment, which can be rented, might have to be treated as specialized equipment. Software that has been developed during the identification phase is considered as bespoke equipment; it must not additionally be considered for in the exploitation phase.

d) **Chip-level attacks equipment**, necessary to implement chip level attacks is generally not widely available on the market and its access is restricted. It is also very expensive, and therefore is considered as a category on its own. Only the following equipment belong to this category:

- Focused Ion Beam
- Scanning Electron Microscope
- Abrasive Laser Equipment

If, for one phase (identification or exploitation), equipment from different levels is required, only the highest level shall be retained.

If the same equipment used for the identification phase can be reused for exploitation, it may not be accounted twice. In such case, the cost of equipment can be divided by two and spread equally over identification and exploitation.

Parts refer to components required to hide the signs of an attack; to otherwise replace components that have been broken during an attack, like a case part, a display or a printer; to created data-monitoring or communicating bug; or otherwise are needed to perform the attack. If the same part may be used for identification and exploitation, it must only be accounted for once.

a) **Standard parts** are readily available to the attacker, either by purchasing them from a supply store or by re-using parts from a mechanical sample of the same device.

b) **Specialized parts** are not readily available to the attacker but could be acquired without undue effort. These might be parts that can be ordered from the stock but require long delivery time or a certain minimum component count for purchase.

c) **Bespoke parts** are not readily available and have to be specifically manufactured. It is very unlikely that an attack requires bespoke spare parts.

Rating Exploitation

It is important to note that only initial exploitation is considered, as further exploitations can reuse equipment, knowledge, and are subject to optimization, which cannot be easily assessed through laboratory evaluations.

The following items in calculation are typically subject to reuse in further exploitation phases:

- Equipment
- Knowledge

If several attack scenarios lead to the same potential in total and exploitation, then the one that has the lowest cost in exploitation, exclusive of the items above, must be considered.

Rating Success of an Attack

If the difficulty of implementation an attack is sufficiently high, resulting in the attack to succeed on a limited number of targets, multiple devices can be considered, given the following limitations.

To reflect this matter of fact, the number of target devices (i.e. functional samples with working keys in the exploitation phase) can be multiplied using the following factors:

Table 2: Success Rate Multiplying Factor

Probability of Success	Factor
$P \geq 0.5$	1
$0.5 > P \geq 0.25$	1.5
$P < 0.25$	2

When determining the probability, each step of the attack must be divided in likely independent phases with a featured probability. The overall probability is obtained by multiplying all factors together.

Proper documentation is required when the overall probability falls under 0.5. Determining the probability is typically based upon experiments with the devices, and may involve proper sampling to obtain meaningful statistical figures.

An Approach to Calculation

The above section identifies the factors to be considered. The table below gives guidelines for the individual factors. When a factor falls close to a boundary, the evaluator should consider use of an intermediate value to those in the table.

For a given attack it might be necessary to make several passes through the table for different attack scenarios (e.g., trading off expertise for time or equipment). The lowest value obtained for these passes should be retained. In the case of a vulnerability that has been identified and is in the public domain, the identifying values should be selected for an attacker to uncover that attack scenario in the public domain, rather than to initially identify it.

Table 3: Attack Potential Factors

Factor	Range	Identification Phase	Exploitation Phase
Attack time	< 1 hour	0	0
	≤ 8 hours	2	2
	≤ 24 hours	3	3
	≤ 40 hours	3.5	3.5
	≤ 80 hours	4	4
	≤ 160 hours	5	5
	Beyond 160 hours	5.5	5.5
Expertise	Layman	0	0
	Proficient	1.5	1.5
	Expert	4	4
Knowledge of the ATM	Public	0	0
	Restricted	2	2
	Sensitive	3	4
Access to the ATM per unit required for the attack. ***Note:*** *If more than one unit is required, the values must be multiplied by the factors given above.*	Mechanical sample	1	1
	Functional samples without working keys	2	2
	Functional sample with working keys and software	4	4
Equipment required for the attack	None	0	0
	Standard	1	1
	Specialized	3	3
	Bespoke	5	5
	Chip-level attacks	7	7
Specific parts required	None	0	0
	Standard	1	1
	Specialized	3	3
	Bespoke	5	5

An approach such as this cannot take account of every circumstance or factor but should give a better indication of the attack potential. Other factors, such as the reliance on unlikely chance occurrences or the likelihood of detection before an attack can be completed, are not included in the basic model but can be used by an evaluator as justification for a rating other than those that the basic model might indicate.

Determining Applicable Time and Levels

For each phase, the testing laboratory shall document all necessary steps, including expertise, equipment, and specific parts needed, time required to operate (in hours), and when relevant, a probability of success.

This information is best summarized in a table containing all the items described above, and helping in the determination of the applicable item for the table.