8 PCI Vorschriften

8.1 Informationen zum PCI Security Standards Council

Das PCI Security Standards Council ist ein internationales, offenes Forum für die Weiterentwicklung, Verbesserung, Archivierung, Verbreitung und Implementierung von Sicherheitsstandards für den Schutz von Kontodaten.

Die Aufgabe des PCI Security Standards Council ist es, durch Information, Weiterbildung und Aufklärung über die PCI Security Standards die Sicherheit von Zahlungs- und Kontodaten zu erhöhen. Die Organisation wurde von American Express, Discover Financial Services, JCB International, MasterCard Worldwide, und Visa, Inc. gegründet. Die offizielle Internetseite ist unter folgendem Link zu finden:

https://de.pcisecuritystandards.org/

8.2 Rückbauschutz

Gemäss der internationalen PCI Vorschrift wurden die einzelnen Komponenten des PayVenSmall Terminals mit einem Rückbauschutz ausgerüstet.

Damit soll verhindert werden, dass Sie während des Betriebs böswillig ausgebaut, modifiziert und wieder in Betrieb genommen werden.

Wichtig!

- Die im Feld ausgebauten Komponenten müssen stets zur PayTec zurückgebracht werden, um wieder reaktiviert zu werden.

8.3 Sichtschutz

Um beim Einbau des PINPads die PCI Konformität zu erfüllen, **muss** die Eingabe des PINs durch einen Sichtschutz geschirmt werden. Die Vorgaben bezüglich Sichtschutzes sind der jeweils aktuellsten Version der vom PCI Security Standards Council LLC herausgegebenen Spezifikationen zu entnehmen (Derived Test Requirements).

In diesem Kapitel ist ein Auszug der Spezifikationen (Appendix A) aus PIN Transaction Security (PTS) Point of Interaction (POI) – Derived Test Requirements Version 5.1 March 2018.

Appendix A: Criteria for the Privacy Screen Design

A.1.1 Upright (for example, Unattended) Privacy Screen Design Criteria to be met by the Device's 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.

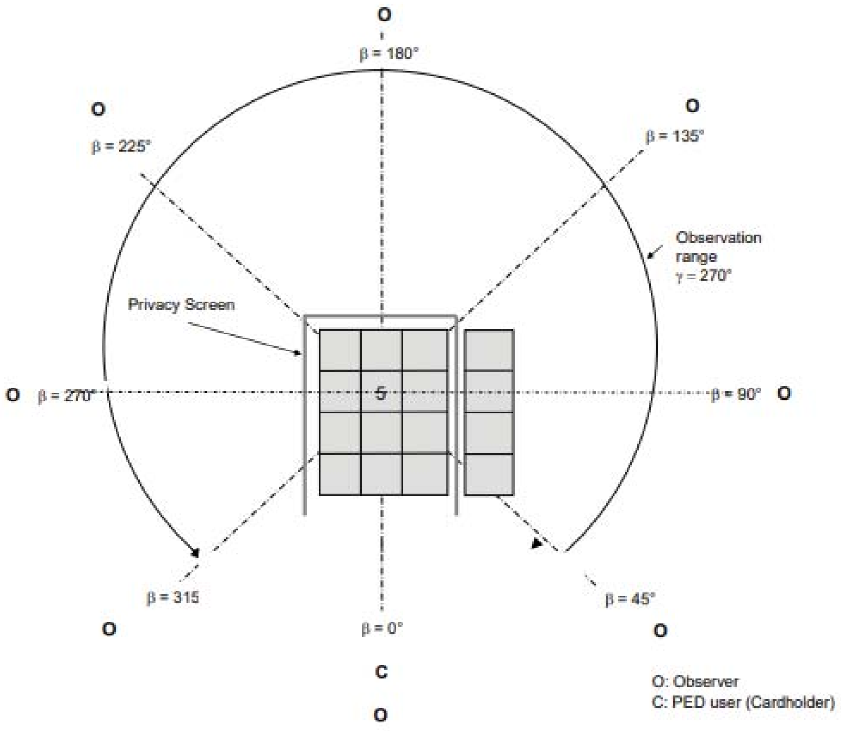


Figure A1: Sample device with privacy screen range, bird's eye view

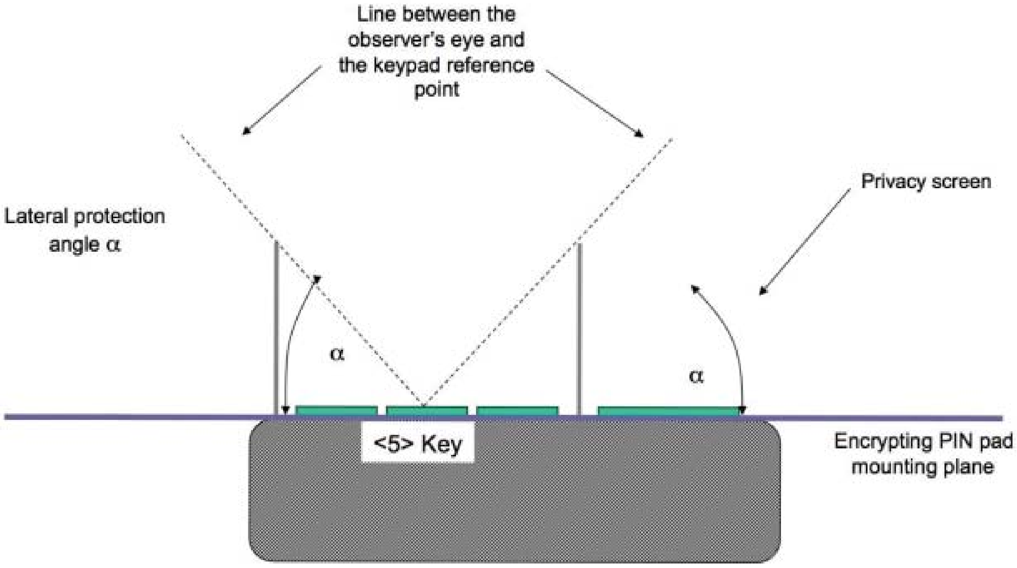

Line between the observer's eye and the keypad reference point
Lateral protection angle α
Privacy screen
α
α
<5> Key
Encrypting PIN pad mounting plane

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

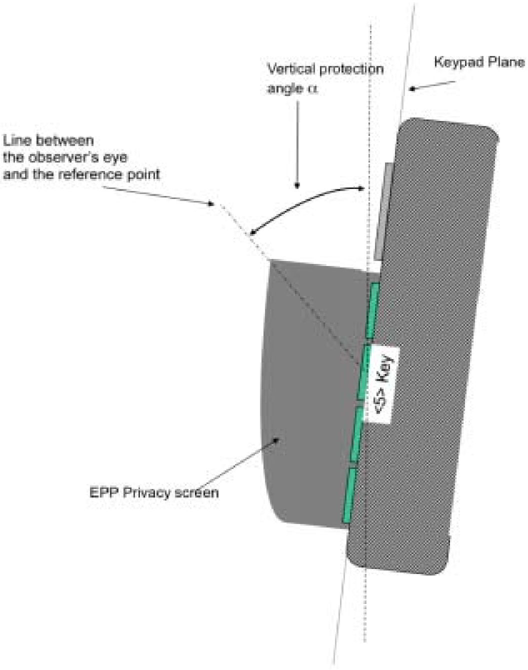
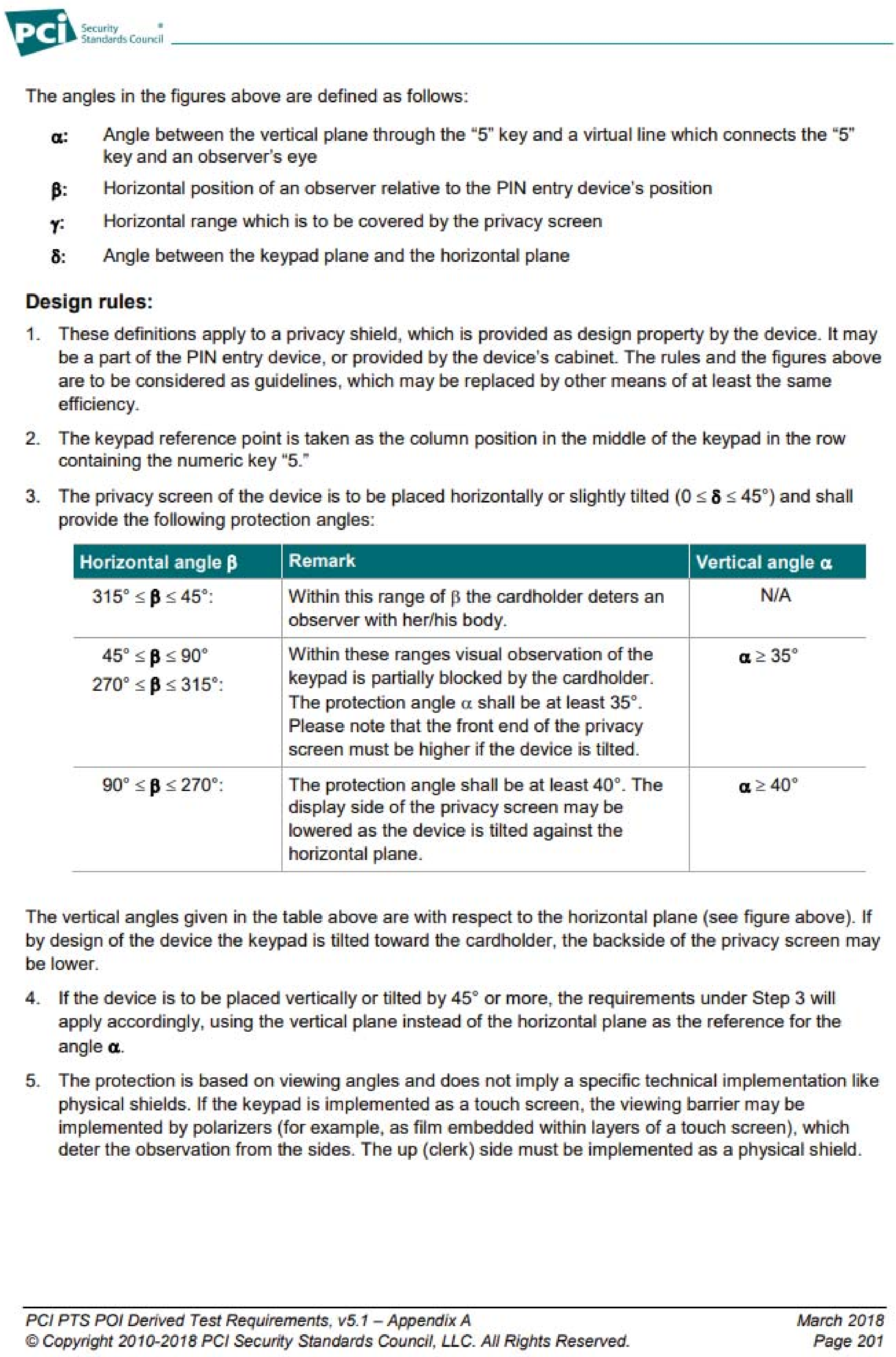

Vertical protection angle α
Keypad Plane
Line between the observer's eye and the reference point
<5> Key
EPP Privacy screen

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 ($0 \leq \boldsymbol{\delta} \leq 45°$) and shall provide the following protection angles:

Horizontal angle $\boldsymbol{\beta}$	Remark	Vertical angle $\boldsymbol{\alpha}$
$315° \leq \boldsymbol{\beta} \leq 45°$:	Within this range of β the cardholder deters an observer with her/his body.	N/A
$45° \leq \boldsymbol{\beta} \leq 90°$ $270° \leq \boldsymbol{\beta} \leq 315°$:	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.	$\boldsymbol{\alpha} \geq 35°$
$90° \leq \boldsymbol{\beta} \leq 270°$:	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.	$\boldsymbol{\alpha} \geq 40°$

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 $\boldsymbol{\alpha}$.
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 (for example, as film embedded within layers of a touch screen), which deter the observation from the sides. The up (clerk) side must be implemented as a physical shield.

A.1.2 Countertop (for example, Attended Device) Privacy Screen Design Criteria to be met by the Device's Design

The following are examples of device's privacy screens being an integral part of the device that are compliant with *PCI PTS POI Security Requirements*. Other designs may also be acceptable.

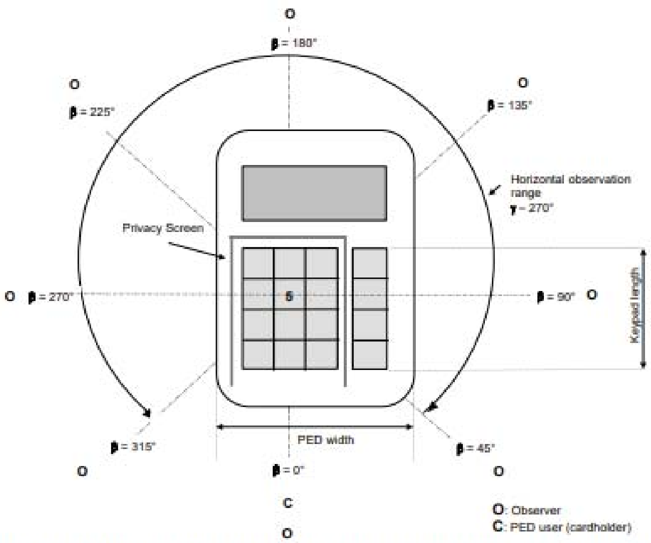


Figure A4: Sample device with privacy screen range, bird's eye view

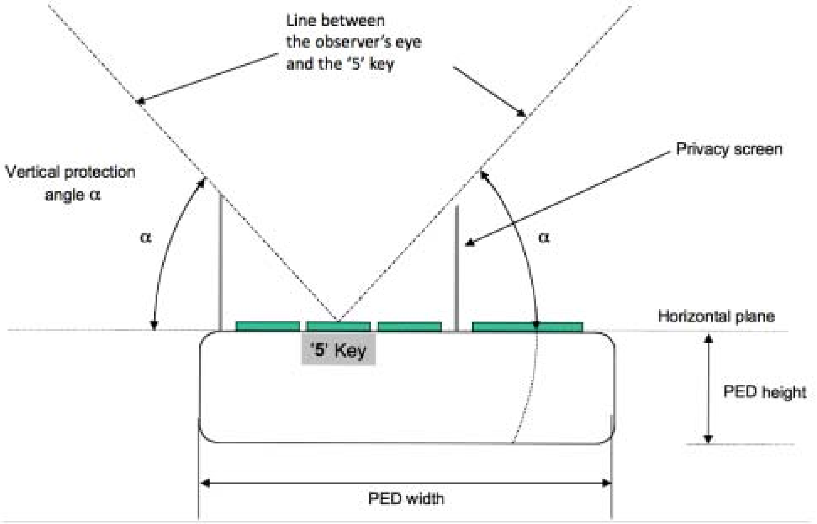

Line between the observer's eye and the '5' key
Privacy screen
Vertical protection angle α
α
α
Horizontal plane
'5' Key
PED height
PED width

Figure A5: Sample device, front side view

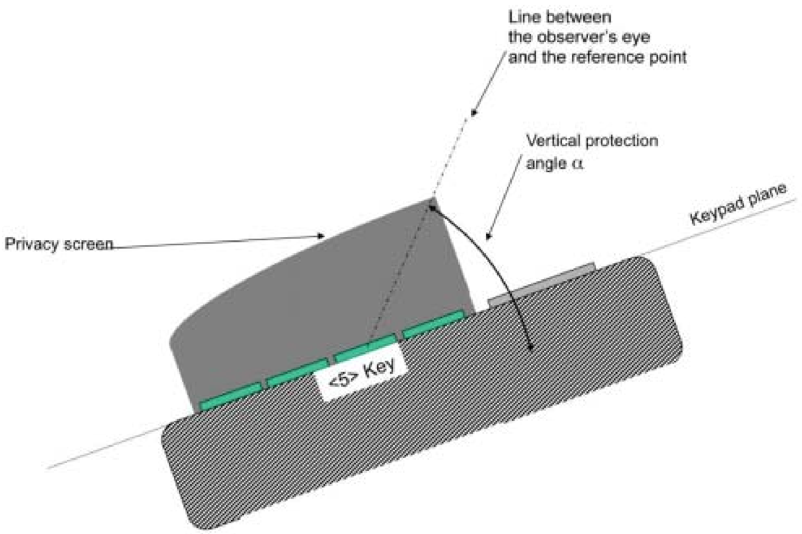
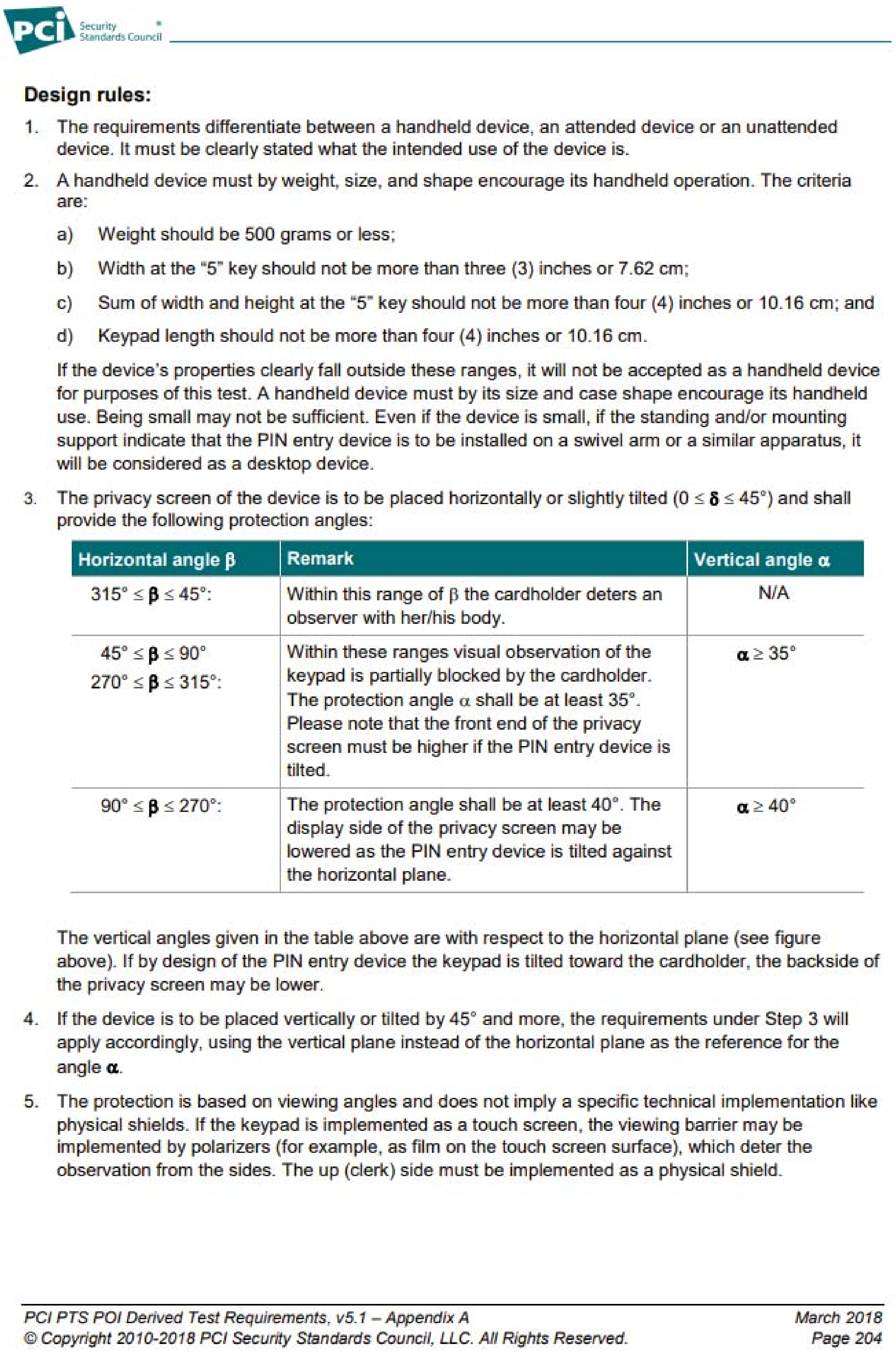


Figure A6: Sample device, side view

The angles in the figures above are defined as follows:

- **α:** Angle between the horizontal 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 user'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. The requirements differentiate between a handheld device, an attended device or an unattended device. It must be clearly stated what the intended use of the device is.
2. A handheld device must by weight, size, and shape encourage its handheld operation. The criteria are:

   a) Weight should be 500 grams or less;

   b) Width at the “5” key should not be more than three (3) inches or 7.62 cm;

   c) Sum of width and height at the “5” key should not be more than four (4) inches or 10.16 cm; and

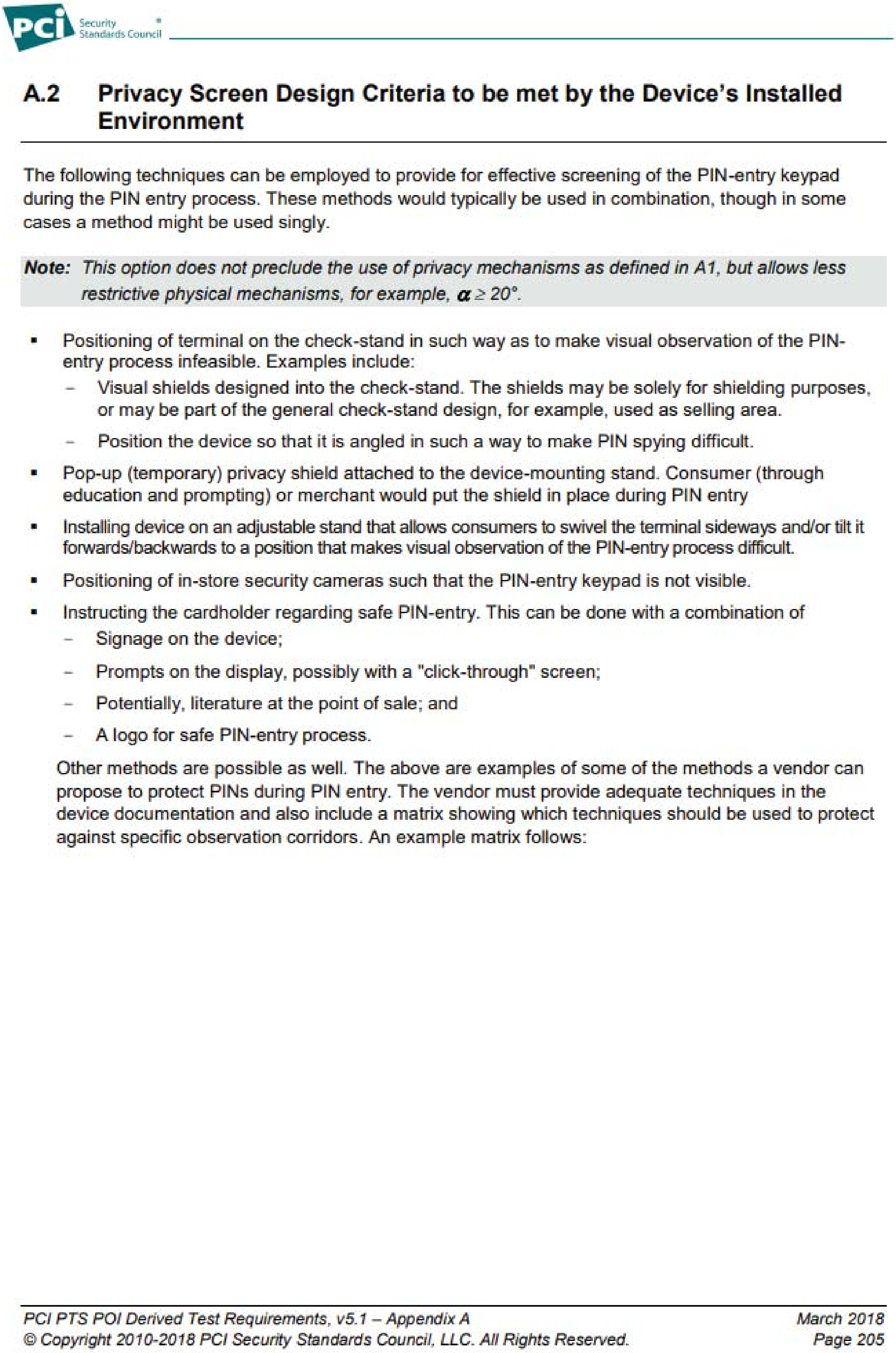
   d) Keypad length should not be more than four (4) inches or 10.16 cm.

   If the device’s properties clearly fall outside these ranges, it will not be accepted as a handheld device for purposes of this test. A handheld device must by its size and case shape encourage its handheld use. Being small may not be sufficient. Even if the device is small, if the standing and/or mounting support indicate that the PIN entry device is to be installed on a swivel arm or a similar apparatus, it will be considered as a desktop device.
3. The privacy screen of the device is to be placed horizontally or slightly tilted ($0 \leq \boldsymbol{\delta} \leq 45°$) and shall provide the following protection angles:

Horizontal angle β	Remark	Vertical angle α
$315° \leq \boldsymbol{\beta} \leq 45°$:	Within this range of β the cardholder deters an observer with her/his body.	N/A
$45° \leq \boldsymbol{\beta} \leq 90°$ $270° \leq \boldsymbol{\beta} \leq 315°$:	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 PIN entry device is tilted.	$\boldsymbol{\alpha} \geq 35°$
$90° \leq \boldsymbol{\beta} \leq 270°$:	The protection angle shall be at least 40°. The display side of the privacy screen may be lowered as the PIN entry device is tilted against the horizontal plane.	$\boldsymbol{\alpha} \geq 40°$

   The vertical angles given in the table above are with respect to the horizontal plane (see figure above). If by design of the PIN entry 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° and more, the requirements under Step 3 will apply accordingly, using the vertical plane instead of the horizontal plane as the reference for the angle $\boldsymbol{\alpha}$.
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 (for example, 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.

PCI PTS POI Derived Test Requirements, v5.1 – Appendix A *March 2018*
© Copyright 2010-2018 PCI Security Standards Council, LLC. All Rights Reserved. *Page 204*



A.2 Privacy Screen Design Criteria to be met by the Device's Installed Environment

The following techniques can be employed to provide for effective screening of the PIN-entry keypad during the PIN entry process. These methods would typically be used in combination, though in some cases a method might be used singly.

Note: *This option does not preclude the use of privacy mechanisms as defined in A1, but allows less restrictive physical mechanisms, for example,* $\alpha \geq 20^\circ$.

- Positioning of terminal on the check-stand in such way as to make visual observation of the PIN-entry process infeasible. Examples include:
  - Visual shields designed into the check-stand. The shields may be solely for shielding purposes, or may be part of the general check-stand design, for example, used as selling area.
  - Position the device so that it is angled in such a way to make PIN spying difficult.
- Pop-up (temporary) privacy shield attached to the device-mounting stand. Consumer (through education and prompting) or merchant would put the shield in place during PIN entry
- Installing device on an adjustable stand that allows consumers to swivel the terminal sideways and/or tilt it forwards/backwards to a position that makes visual observation of the PIN-entry process difficult.
- Positioning of in-store security cameras such that the PIN-entry keypad is not visible.
- Instructing the cardholder regarding safe PIN-entry. This can be done with a combination of
  - Signage on the device;
  - Prompts on the display, possibly with a "click-through" screen;
  - Potentially, literature at the point of sale; and
  - A logo for safe PIN-entry process.

  Other methods are possible as well. The above are examples of some of the methods a vendor can propose to protect PINs during PIN entry. The vendor must provide adequate techniques in the device documentation and also include a matrix showing which techniques should be used to protect against specific observation corridors. An example matrix follows:

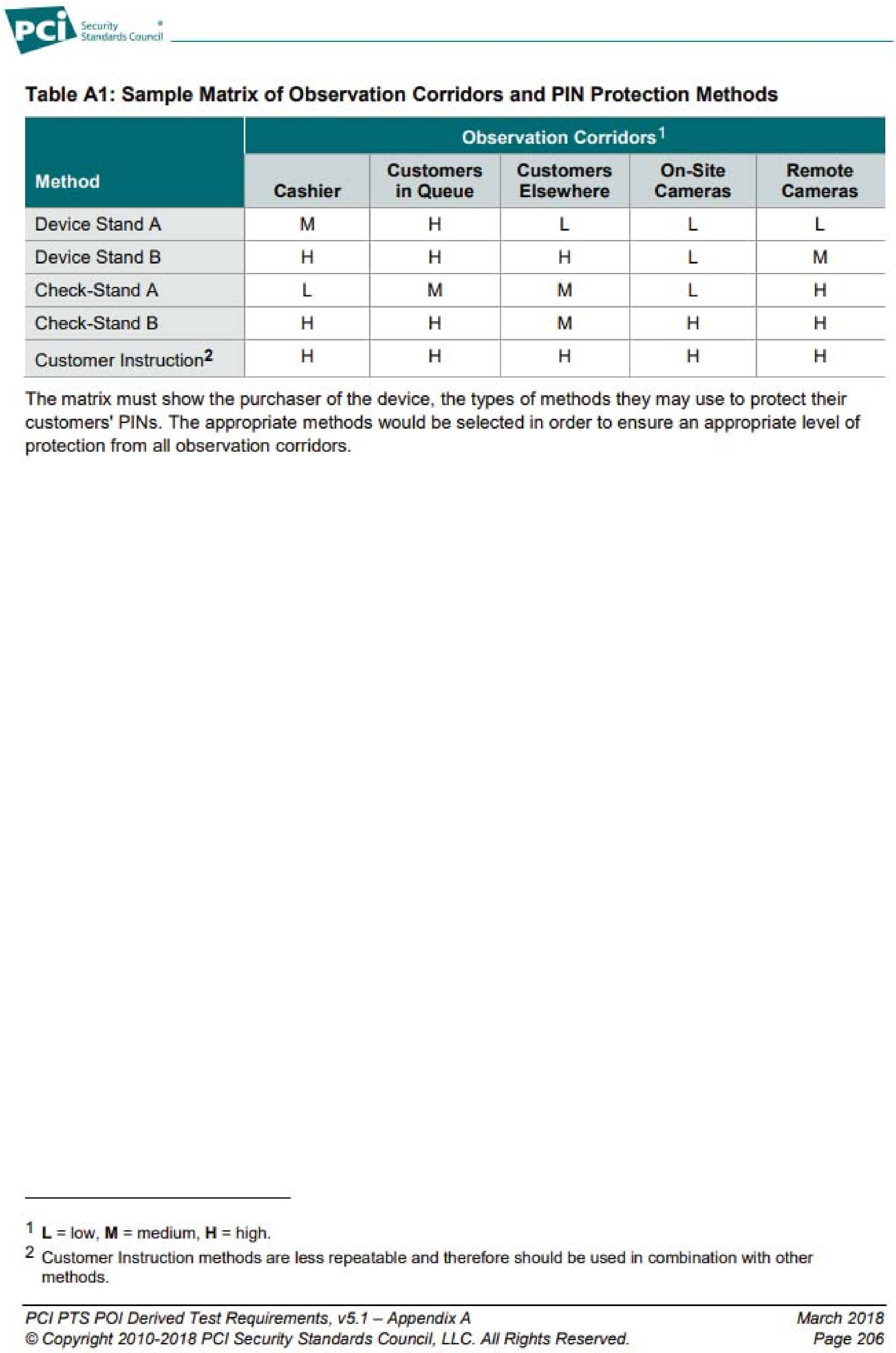


Table A1: Sample Matrix of Observation Corridors and PIN Protection Methods

Method	Observation Corridors[1]				
	Cashier	Customers in Queue	Customers Elsewhere	On-Site Cameras	Remote Cameras
Device Stand A	M	H	L	L	L
Device Stand B	H	H	H	L	M
Check-Stand A	L	M	M	L	H
Check-Stand B	H	H	M	H	H
Customer Instruction[2]	H	H	H	H	H

The matrix must show the purchaser of the device, the types of methods they may use to protect their customers' PINs. The appropriate methods would be selected in order to ensure an appropriate level of protection from all observation corridors.

[1] **L** = low, **M** = medium, **H** = high.

[2] Customer Instruction methods are less repeatable and therefore should be used in combination with other methods.