Adsigo

Info-Veranstaltung PCI DSS

Wirtschaftskammer Wien

21. Juni 2017

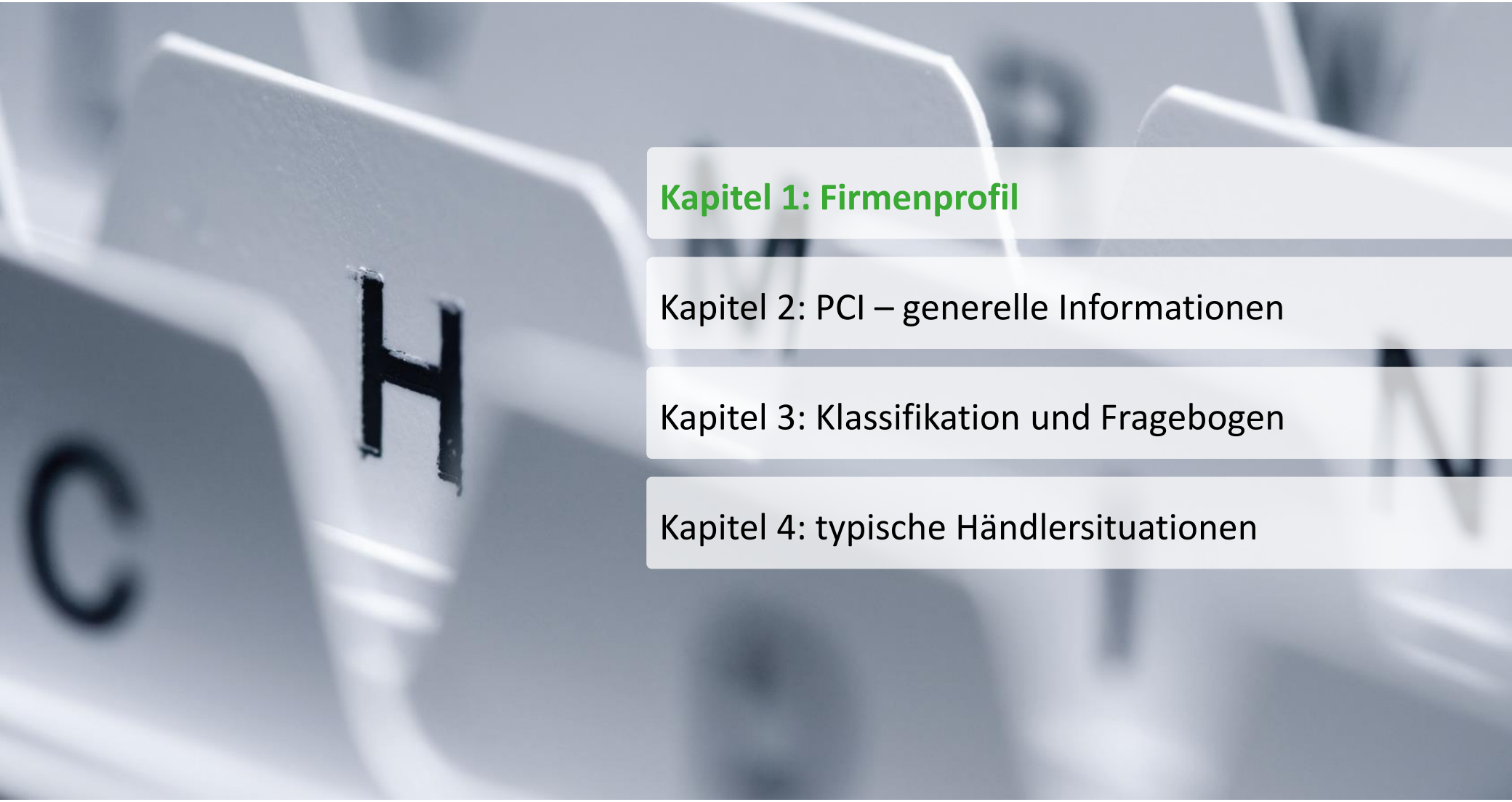
Adsigo
Compliance • Governance • Information Security

Ralph Wörn
Vorstand / CEO

Adsigo AG
Königsallee 43
71638 Ludwigsburg
Germany
www.adsigo.com

+49 176 123 50900 (mobile)
ralph.woern@adsigo.com

Inhalt



Firmenprofil

Standorte

Firmensitz Ludwigsburg, Deutschland

Weitere Standorte:

- Hamburg, Deutschland (Adsigo AG)
- Zürich, Schweiz (Adsigo AG)
- Ulm, Deutschland (Partner)
- Zagreb, Kroatien (Partner)

Dienstleistungs-Portfolio

PCI Compliance Audits und Zertifizierung

PCI Vorbereitungs- und Beratungsleistungen

PCI Workshops, Training & Awareness Schulungen

Penetrationstest, Schwachstellen-Scans, IT-Forensik

BDSG Datenschutz Audits, externer Datenschutzbeauftragter, Beratungs-leistungen

ISO 27001 Vorbereitungs- und Beratungs-dienstleistungen

eDiscovery Untersuchungen

PCI Dienstleistungen

Akkreditierung für die Regionen Europe und CEMEA

Partner für Banken, Acquirer, Issuer, Prozessoren, Service Provider und Händler

Umfassendes Dienstleistungsangebot für alle Phasen der PCI-Compliance

- Vorbereitung auf die PCI-Compliance
- Vor-Audits und Gap Analysen
- Compliance-Beratung und Unterstützung
- Erst-Zertifizierung und regelmäßige Re-Zertifizierung

Mitarbeiter-Skills

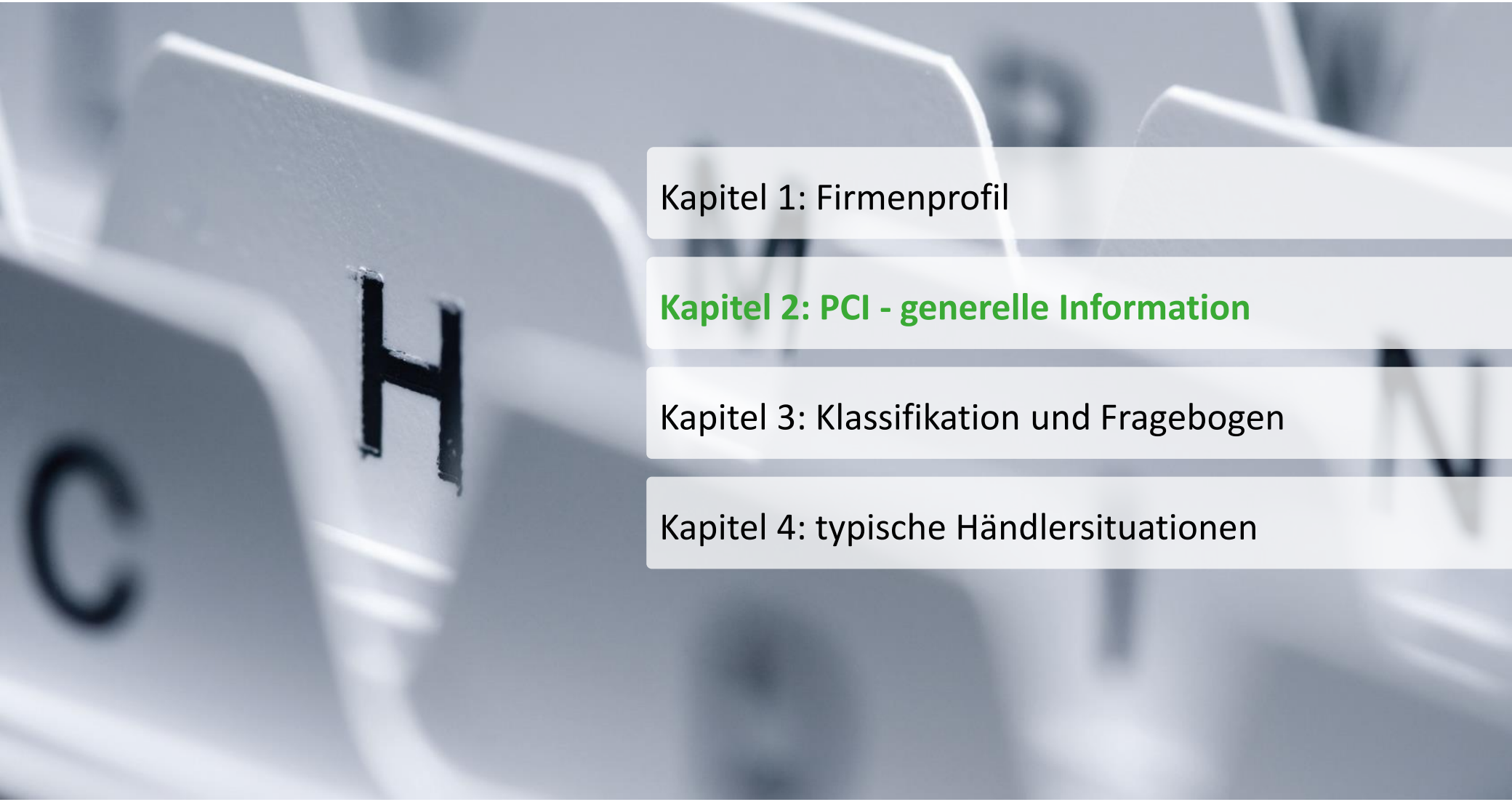
Langjährige Audit- und Consultingerfahrung der Mitarbeiter in den unterschiedlichen PCI-Standards (PCI DSS, PA-DSS, P2PE, PIN Security, PNC, Verified by Visa, u.a.)

Mehr als 700 durchgeführte Assessments durch unsere erfahrenen Auditoren (QSA) in den letzten 10 Jahren

Umfassende Branchenerfahrung der Mitarbeiter im Paymentsektor

Umfassende IT-Security Qualifikationen der Mitarbeiter (CISA, CISM, CRISC, ISO 27001, BDSG)

Inhalt

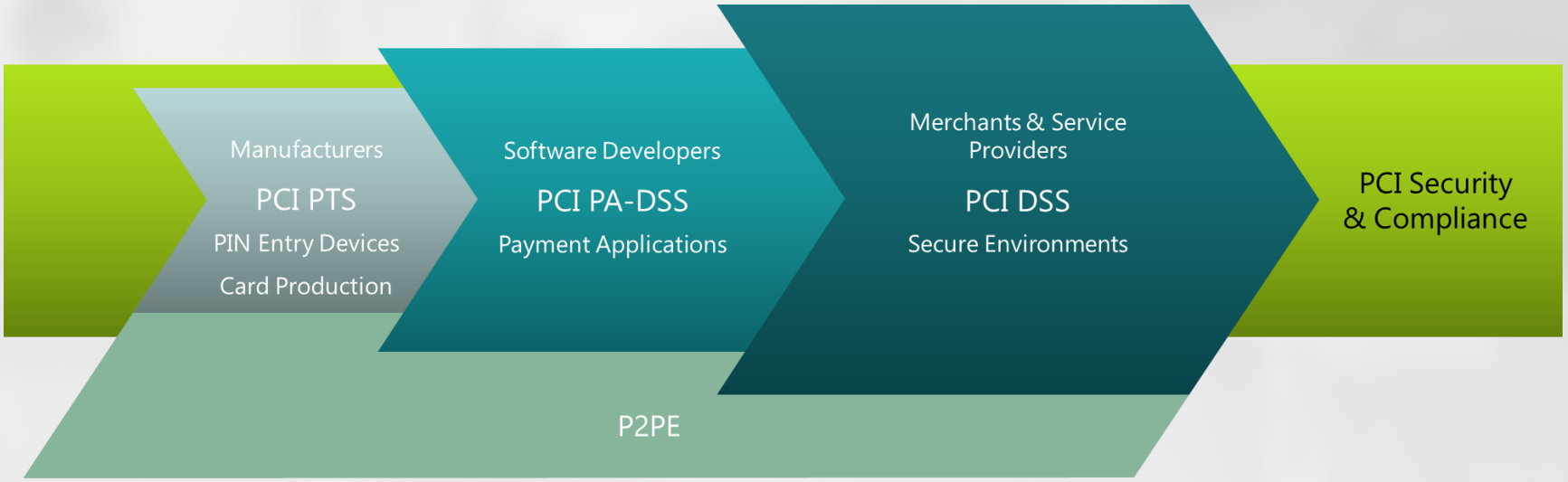


Organisationen

Definiert und beaufsichtigt die PCI Standards weltweit akkreditiert und prüft die Zertifizierer

Kartenorganisationen beziehen sich in ihren Sicherheitsprogrammen auf die PCI-Anforderungen

PCI Standards



Quelle: PCI SSC

PCI Standards

PCI DSS – ein globaler Sicherheitsstandard

- anzuwenden durch alle Unternehmen die Kartendaten verarbeite, übertragen oder speichern
- Anforderungen gelten weltweit

Zielgruppen für die Umsetzung

- Händler
- Dienstleister und Hersteller eines Händlers, die direkt oder indirekt an der Zahlungsabwicklung beteiligt sind, wie z.B. Payment Service Provider, Softwarehersteller, Zahlungsterminalhersteller, Rechenzentren, Call Center, Hosting Dienstleister, etc.

Inhalt

Zusammenhang zwischen Klassifikation und Fragebogen

Klassifikation dient zur Feststellung in welche Gruppe der Händler einzuordnen ist, um
- die Zertifizierungsanforderungen zu bestimmen
- den Fragebogen-Typ zu bestimmen
- die Notwendigkeit einer externen Auditierung zu ermitteln

Wesentliche Entscheidungskriterien sind:
- Jährliche Transaktionszahl
- Akzeptanzkanäle
- Outsourcing oder Eigenverarbeitung von Transaktionsdaten

Wieviel Transaktionen verarbeite ich jährlich?

Adsigo
Compliance • Governance • Information Security

	für MasterCard & Maestro	für Visa
Mehr als 6 Millionen Transaktionen jährlich über alle Akzeptanzkanäle	Level 1	Level 1
Zwischen 1 Million und 6 Millionen Transaktionen jährlich über alle Akzeptanzkanäle	Level 2	Level 2
Bis zu 1 Million nicht-eCommerce Transaktionen jährlich	Level 4	Level 4
Zwischen 20.000 und 1 Million eCommerce Transaktionen jährlich	Level 3	Level 3
Weniger als 20.000 eCommerce Transaktionen jährlich	Level 4	Level 4

Mein Level:

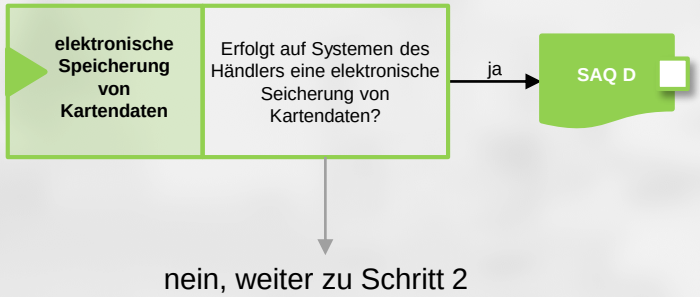
Über welche Kanäle erhalte ich Kartendaten?

Arten von Akzeptanzkanälen

card-present Transaktionen	via eines Zahlungsterminals
mail order / telephone order	papierbasierend
Manuelle PAN-Eingabe am Terminal	papierbasierend
e-Commerce	

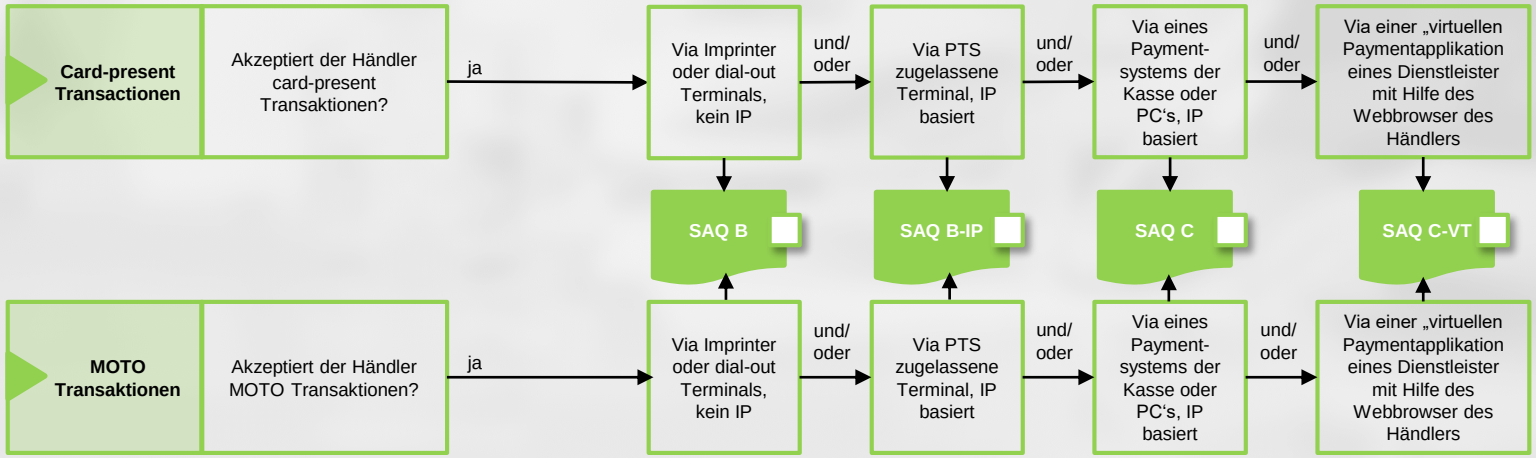
Welcher SAQ-Fragebogen ist für mich zutreffend?

Schritt 1:



Welcher SAQ-Fragebogen ist für mich zutreffend?

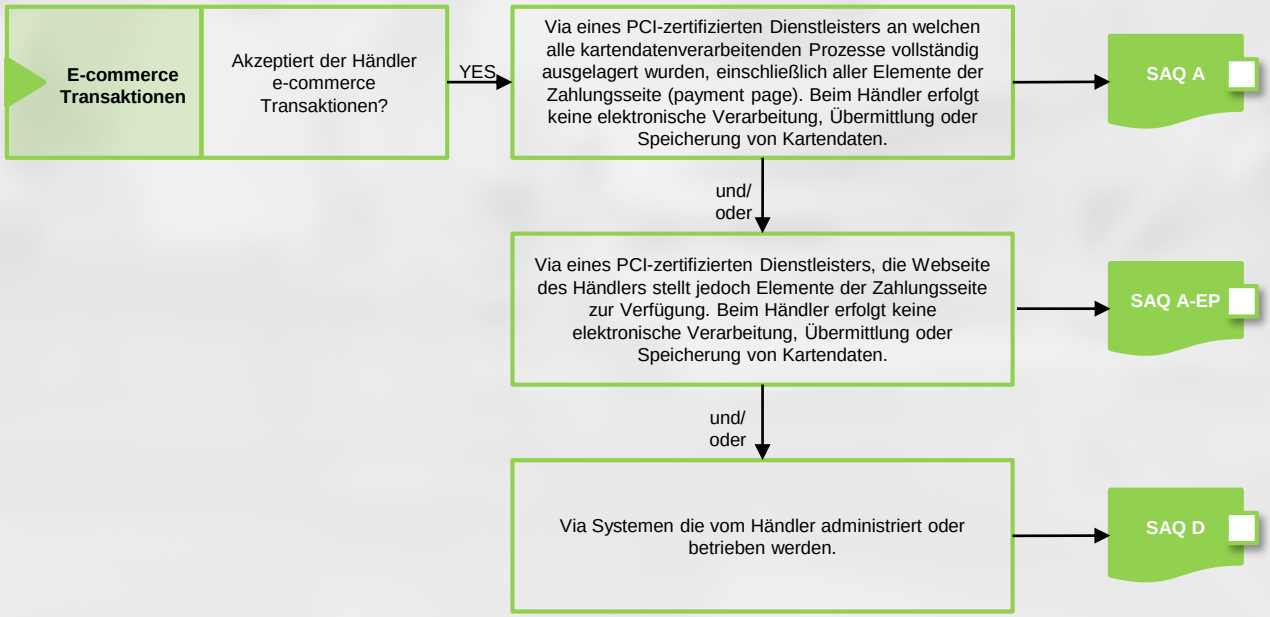
Schritt 2:



⟹ weiter zu Schritt 3

Welcher SAQ-Fragebogen ist für mich zutreffend?

Schritt 3:



Zusammenfassung

Mein Level:

Meine Fragebögen (SAQ):

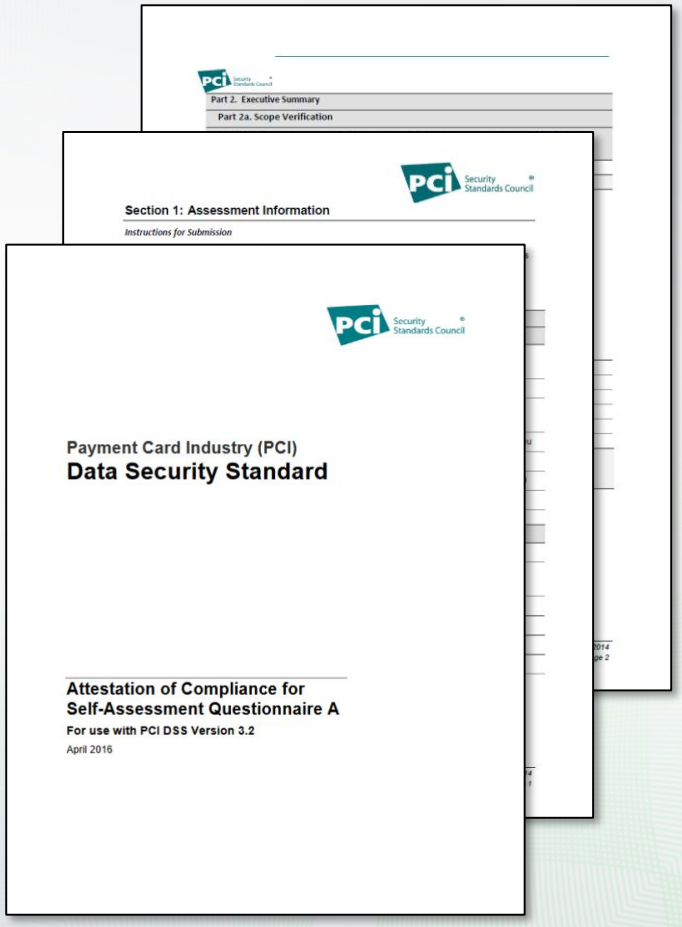
Was muss ich für eine Zertifizierung tun?

Übersicht zu den Validierungsanforderungen

Level 1	• Report on Compliance (Auditbericht) durch einen Auditor erstellt • vierteljährliche Schwachstellen-Scans
Level 2	• SAQ durch einen internen ISA (MasterCard-Anforderung) • oder Report on Compliance (Auditbericht) durch einen Auditor erstellt • vierteljährliche Schwachstellen-Scans
Level 3	• SAQ durch einen internen Verantwortlichen • vierteljährliche Schwachstellen-Scans
Level 4 (Acquirer-spezifisch)	• SAQ durch einen internen Verantwortlichen • vierteljährliche Schwachstellen-Scans

Compliance Dokumente

Adsigo
Compliance • Governance • Information Security



Selbstauskunft

Auditierung durch QSA

Typische Situationen

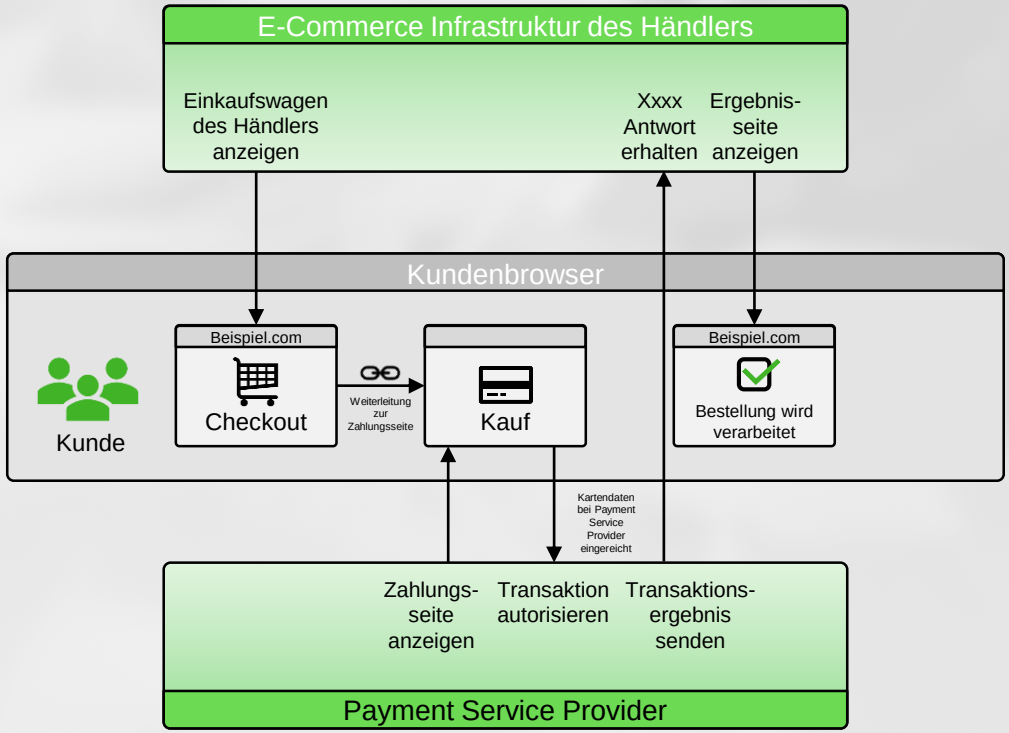
eCommerce Auftritt – Webshop (SAQ A)

Kartenterminal im Geschäft (SAQ B)

Fall 1: eCommerce (Distanzgeschäft) mit Outsourcing an Payment Service Provider

Händler verarbeitet keine Kartendaten elektronisch auf seinen Systemen

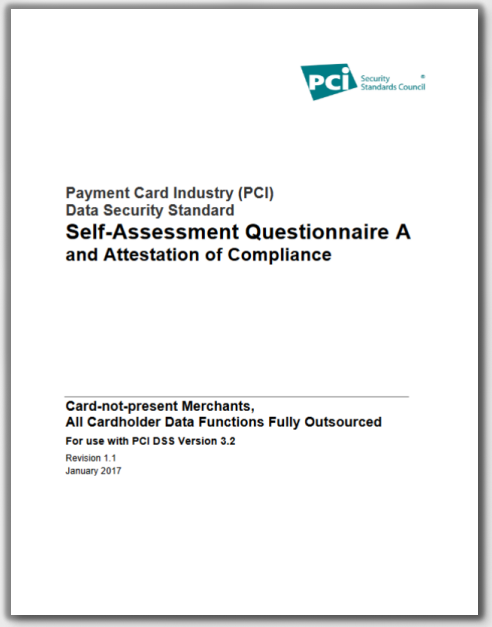
- Nutzung eines iFrames
- Nutzung eines redirect

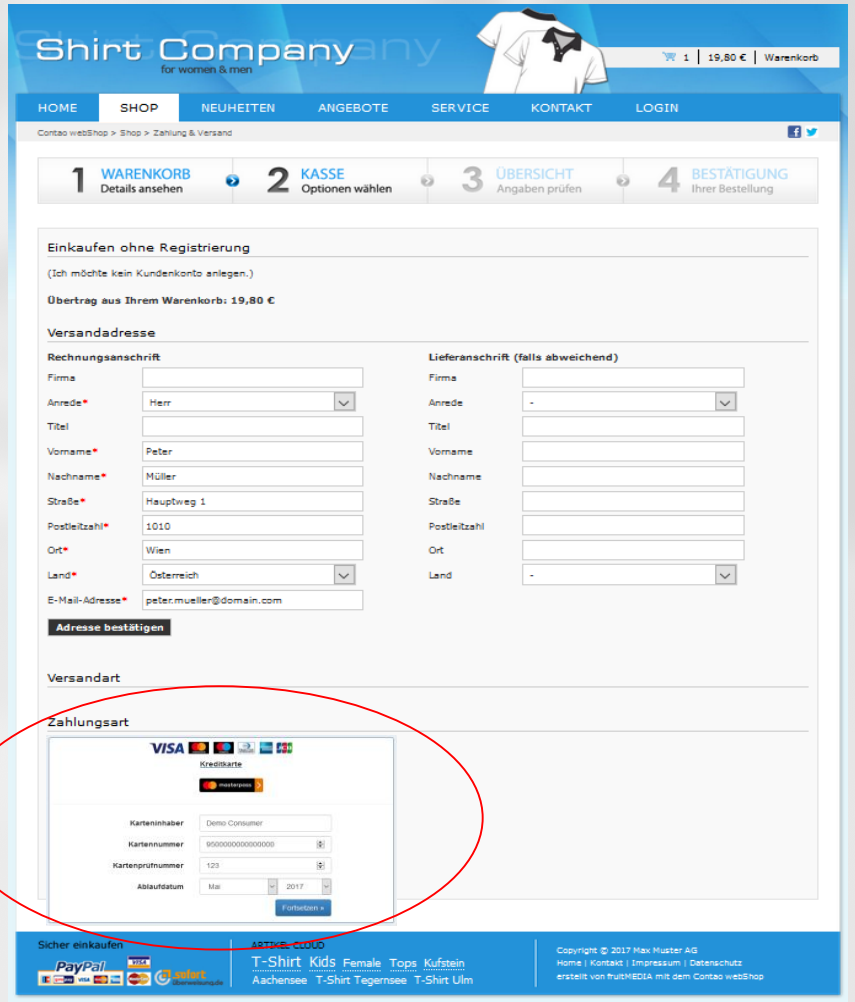


Fall 1: eCommerce (Distanzgeschäft) mit Outsourcing an Payment Service Provider

Adsigo
Compliance • Governance • Information Security

iFrame des Service Providers

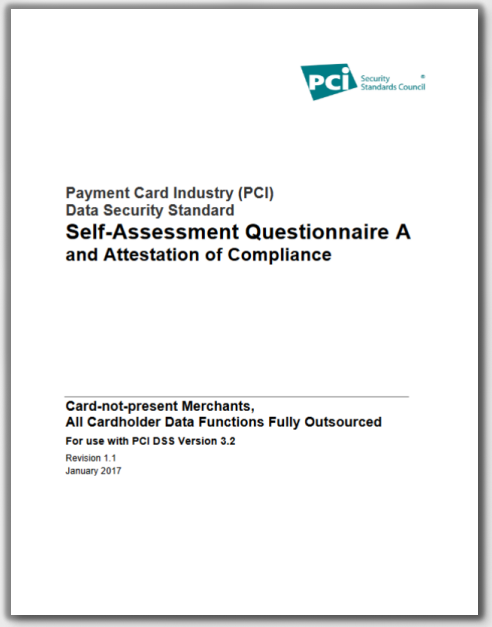


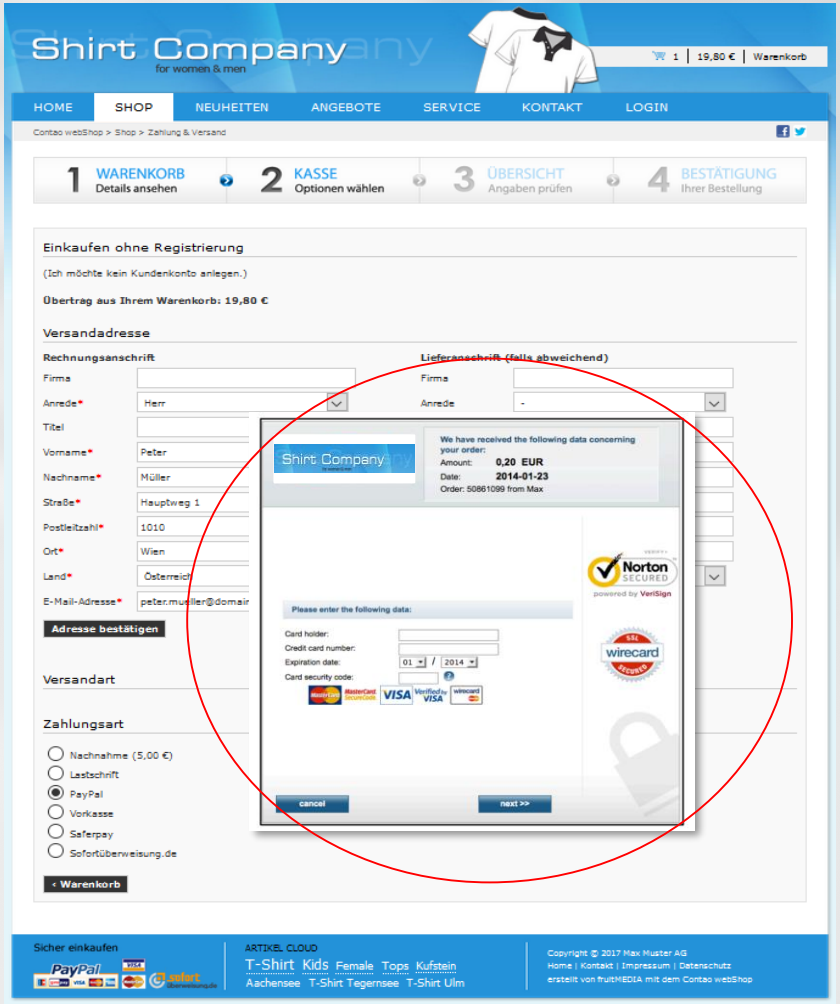


Fall 1: eCommerce (Distanzgeschäft) mit Outsourcing an Payment Service Provider

Adsigo
Compliance • Governance • Information Security

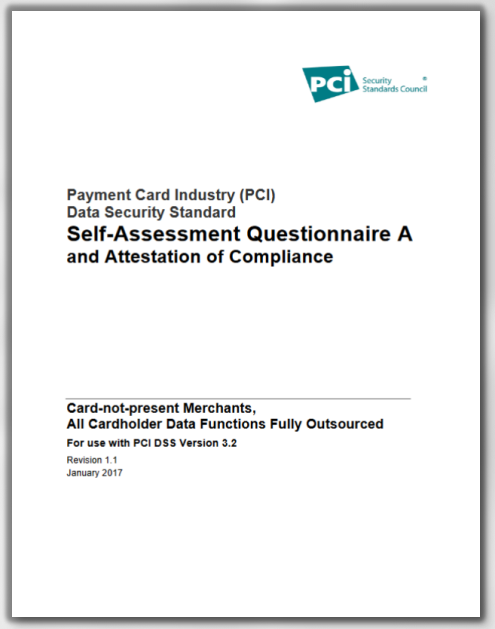
Payment Page des Service Providers (redirect)





SAQ A für eCommerce

- 22 Fragen
- Im Wesentlichen organisatorischen Regelungen und Dokumentationsanforderungen



Kriterien für die Anwendbarkeit dieses SAQ sind:

- nur für „card-not-present“ Transaktionen
- alle transaktionsbezogene Verarbeitung ist vollständig an den Dienstleister ausgelagert
- auf eigenen Systemen erfolgt keine Verarbeitung, Übertragung oder Speicherung von Kartendaten
- der Dienstleister ist PCI-zertifiziert
- Kartendaten liegen maximal in Papierform im eigenen Unternehmen vor (am besten aber gar nicht!), keinesfalls elektronisch
- Im Falle von eCommerce-Transaktionen werden alle Elemente der Zahlungsseite vom Dienstleister bereitgestellt

Typische Situationen

eCommerce Auftritt – Webshop (SAQ A)

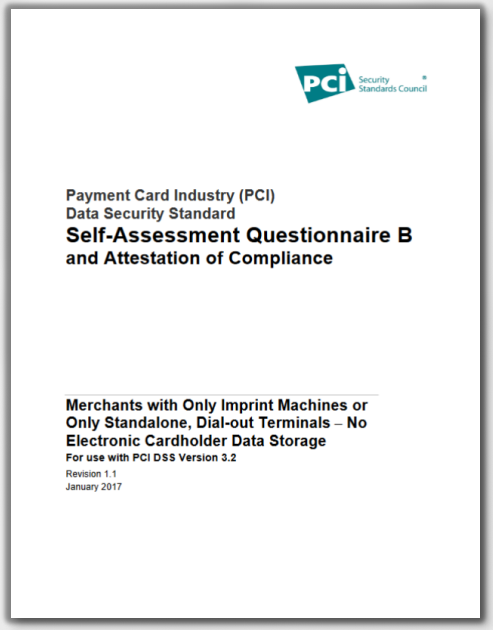
Kartenterminal im Geschäft (SAQ B)

Fall 2: Reisebüro mit Kartenterminal (Präsenz-Zahlung)

Fall 2: Reisebüro mit Kartenterminal (Präsenz-Zahlung)

Adsigo
Compliance • Governance • Information Security

Präsenzzahlung mit einem Kartenterminal via einer Dial-Out-Verbindung



Anbindung über Dial-Out-Verfahren

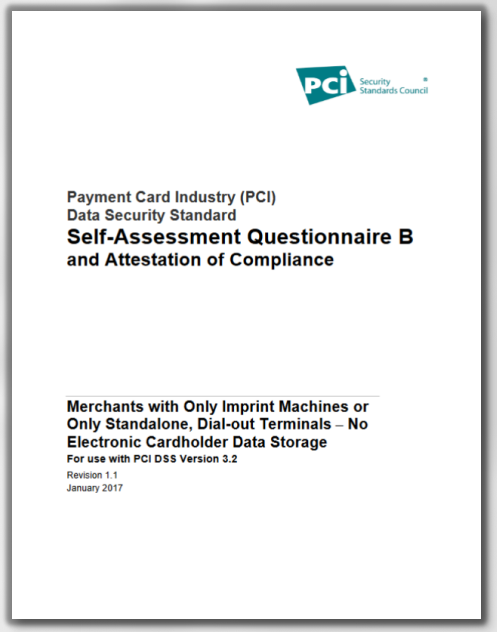
Acquirer

SAQ B für Terminal mit Dial-Out-Anbindung

- 41 Fragen
- organisatorischen Regelungen, Dokumentations-anforderungen, Terminalverwaltung und -sicherheit

Kriterien für die Anwendbarkeit dieses SAQ sind:

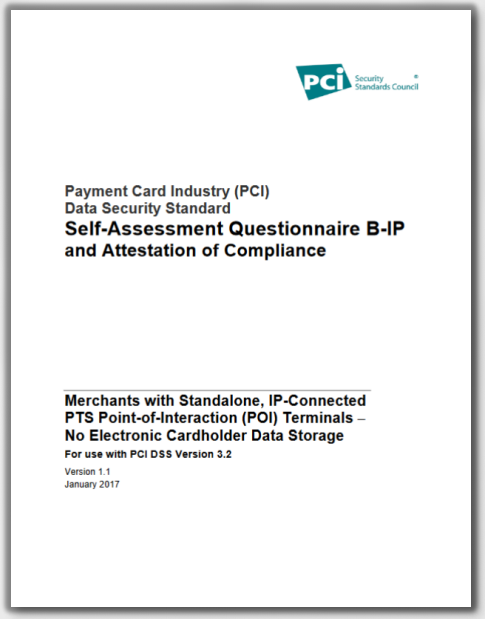
- nur für „dial-out“-Terminals oder Imprinter
- Terminal haben keine Verbindung zu anderen Systemen und sind nicht über IP angebunden
- Kartendaten werden nicht über unternehmenseigene Netzwerke (weder intern noch extern) transportiert
- Kartendaten liegen maximal in Papierform im eigenen Unternehmen vor (am besten aber gar nicht!), keinesfalls elektronisch



Fall 2: Reisebüro mit Kartenterminal (Präsenz-Zahlung)

Adsigo
Compliance • Governance • Information Security

Präsenzzahlung mit einem Kartenterminal via einer IP-Verbindung



Anbindung
über IP

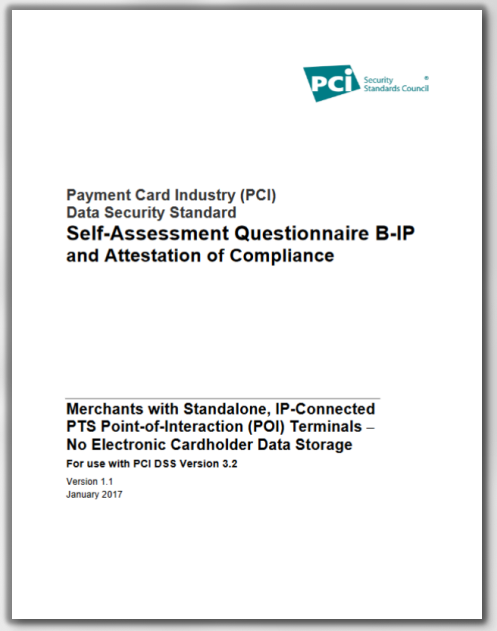
Acquirer

SAQ B-IP für Terminal mit IP-Anbindung

- 86 Fragen
- Externe Schwachstellen-Scans
- organisatorischen Regelungen, Dokumentations-anforderungen, Terminalverwaltung und –sicherheit, technische Sicherheit (Firewalls, Zugriffskontrollen, Konfigurations- und Schwach-stellenmanagement, Transportverschlüsselung)

Kriterien für die Anwendbarkeit dieses SAQ sind:

- Nutzung von PTS-zugelassenen Terminals via IP-Verbindung
- Terminal haben keine Verbindung zu anderen Systemen oder sind von diesen segmentiert
- Kartendaten werden direkt vom Terminal zum Prozessor geschickt
- Kartendaten liegen maximal in Papierform im eigenen Unternehmen vor (am besten aber gar nicht!), keinesfalls elektronisch


Payment Card Industry (PCI)
Data Security Standard
Self-Assessment Questionnaire B-IP and Attestation of Compliance

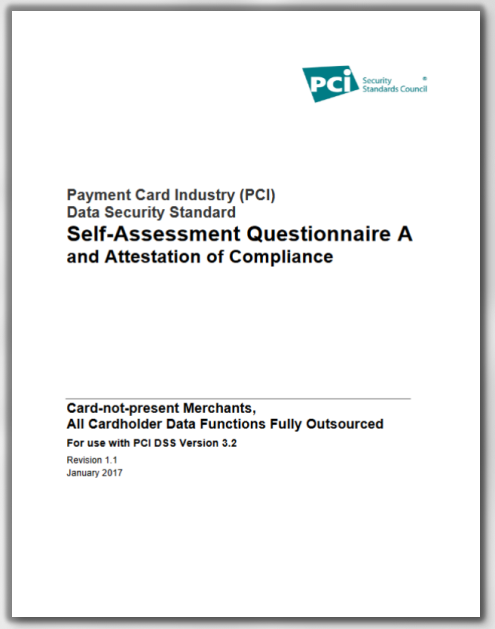
Merchants with Standalone, IP-Connected PTS Point-of-Interaction (POI) Terminals – No Electronic Cardholder Data Storage
For use with PCI DSS Version 3.2
Version 1.1
January 2017

Adsigo
Compliance • Governance • Information Security

Selbstauskunfts-Fragebogen (SAQ A)

SAQ A für eCommerce

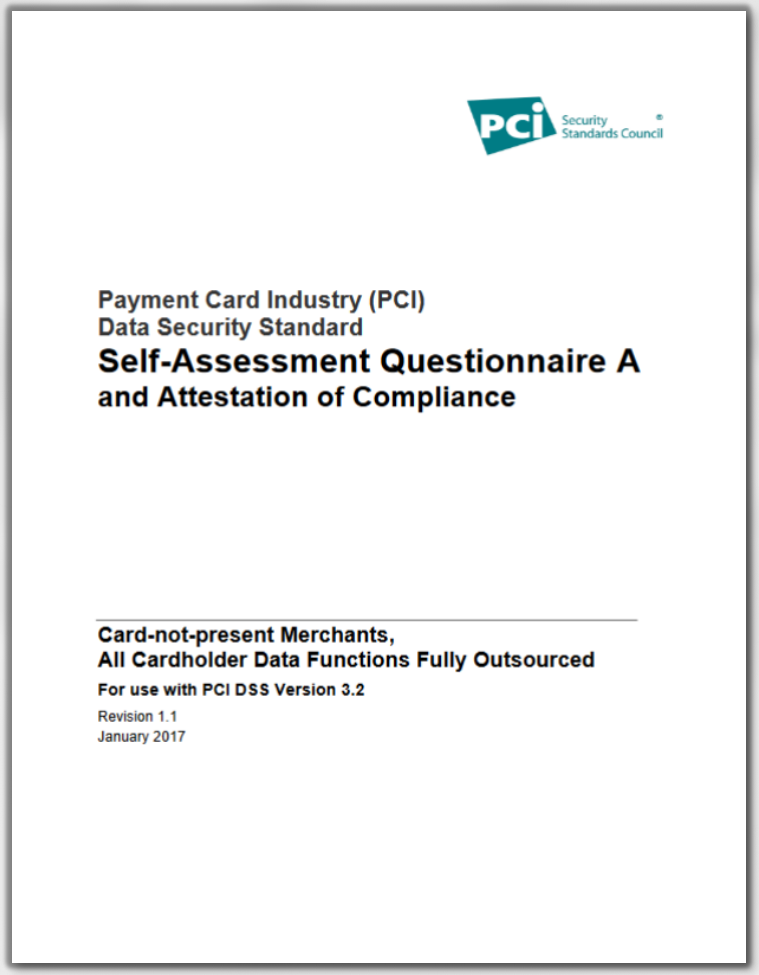
- 22 Fragen
- Im Wesentlichen organisatorischen Regelungen und Dokumentationsanforderungen



Kriterien für die Anwendbarkeit dieses SAQ sind:

- nur für „card-not-present“ Transaktionen
- alle transaktionsbezogene Verarbeitung ist vollständig an den Dienstleister ausgelagert
- auf eigenen Systemen erfolgt keine Verarbeitung, Übertragung oder Speicherung von Kartendaten
- der Dienstleister ist PCI-zertifiziert
- Kartendaten liegen maximal in Papierform im eigenen Unternehmen vor (am besten aber gar nicht!), keinesfalls elektronisch
- Im Falle von eCommerce-Transaktionen werden alle Elemente der Zahlungsseite vom Dienstleister bereitgestellt

SAQ A für eCommerce



Payment Card Industry (PCI)
Data Security Standard

Self-Assessment Questionnaire A
and Attestation of Compliance

Card-not-present Merchants,
All Cardholder Data Functions Fully Outsourced

For use with PCI DSS Version 3.2

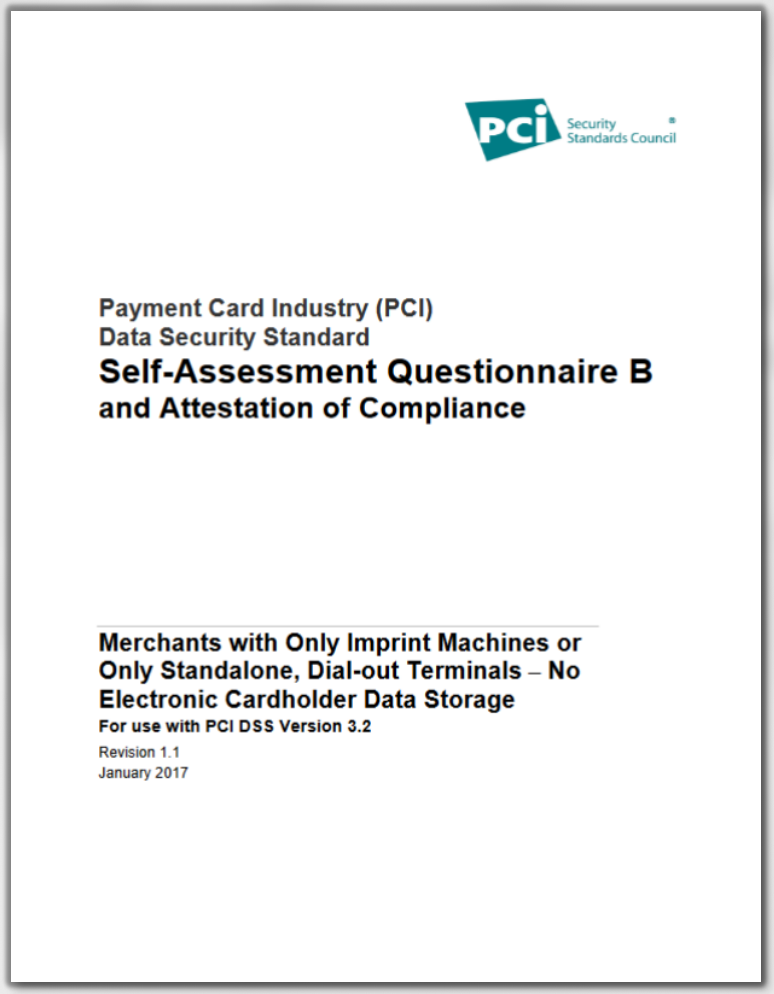
Revision 1.1
January 2017

siehe Hand-Out

Adsigo
Compliance • Governance • Information Security

Selbstauskunfts-Fragebogen (SAQ B)

SAQ B für Terminal mit Dial-Out-Anbindung



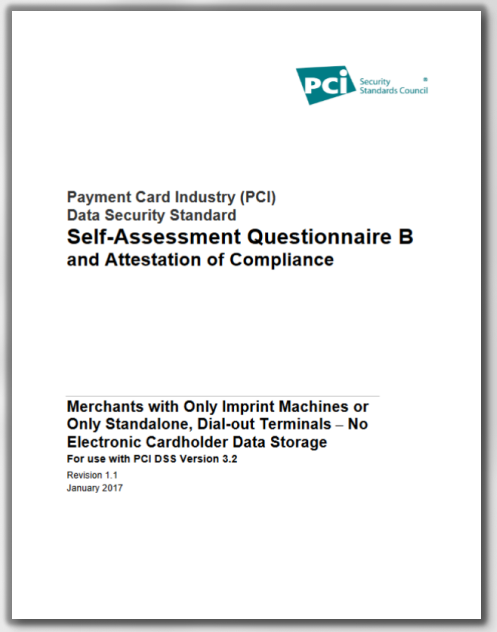
siehe Hand-Out

SAQ B für Terminal mit Dial-Out-Anbindung

- 41 Fragen
- organisatorischen Regelungen, Dokumentations-anforderungen, Terminalverwaltung und -sicherheit

Kriterien für die Anwendbarkeit dieses SAQ sind:

- nur für „dial-out“-Terminals oder Imprinter
- Terminal haben keine Verbindung zu anderen Systemen und sind nicht über IP angebunden
- Kartendaten werden nicht über unternehmenseigene Netzwerke (weder intern noch extern) transportiert
- Kartendaten liegen maximal in Papierform im eigenen Unternehmen vor (am besten aber gar nicht!), keinesfalls elektronisch



Adsigo
Compliance • Governance • Information Security

Zertifizierung

Klassifizierung (Level und Fragebogen)

Klärung ob alle PCI-Anforderungen umgesetzt sind

Ausfüllung des SAQ-Fragebogens oder Durchführung eines Audits

ggfs. Durchführung von Schwachstellen-Scans

Bereitstellung der Complianceunterlagen

Links zu weiteren Informationen

PCI Council Website

www.pcisecuritystandards.org

Dokumenten-Archiv des PCI Council

www.pcisecuritystandards.org//document_library

“Securing the
future of payments together.”

PCI COUNCIL

Adsigo

Vielen Dank für Ihre Aufmerksamkeit

Adsigo
Compliance • Governance • Information Security

Ralph Wörn
Vorstand / CEO

+49 176 123 50900 (mobile)
ralph.woern@adsigo.com

Adsigo AG
Königsallee 43
71638 Ludwigsburg
Germany
www.adsigo.com