

**Informationen und Hinweise für
Händler
zur Umsetzung der Programme**

**MasterCard Site Data Protection (SDP)
und
Visa Account Information Security (AIS)**



**unter Berücksichtigung des
Payment Card Industry (PCI) Data Security Standard**

von

**SRC Security Research & Consulting GmbH
Graurheindorfer Str.149a
53117 Bonn**

1 Einleitung

Die Kreditkartenorganisationen MasterCard International und Visa International haben angesichts der steigenden Missbrauchsraten bei der Nutzung von Kreditkarten die Programme **MasterCard Site Data Protection (SDP)** und **Visa Account Information Security (AIS)** initiiert, um die Sicherheit bei der Speicherung, Verarbeitung und/oder Weiterleitung von Kartendaten zu verbessern. Die Kreditkartenorganisationen haben die Acquirer aufgefordert, den Nachweis zu erbringen, dass Händler und deren Service Provider angemessene technische und organisatorische Sicherheitsmaßnahmen getroffen haben, die eine Kompromittierung von Kartendaten wirksam verhindern.

Die Programme richten sich dementsprechend ausschließlich an Händler und Service Provider, **die Kreditkartendaten selber speichern, verarbeiten und/oder weiterleiten**. Händler, die sich dazu eines Payment Service Providers bedienen, sind von der Umsetzung nicht betroffen.

Im Falle einer Kompromittierung von Kartendaten bei einem Händler (E-Commerce, MOTO und POS) drohen dem Acquirer empfindliche Konventionalstrafen, sollte dieser nicht nachweisen können, dass der angeschlossene Händler bzw. dessen Service Provider diesen Sicherheitsstandards genügt. Daher sind Händler und deren Service Provider aufgefordert, den Nachweis zu erbringen, dass angemessene technische und organisatorische Maßnahmen zum Schutz vor Angriffen und Kompromittierung von Kartendaten, Transaktions- oder Konteninformationen getroffen wurden. Acquirer, deren Händler die Anforderungen der Programme erfüllen, wird im Falle der Kompromittierung von Zahlungsverkehrsdaten eine teilweise oder vollständige Befreiung von den Strafen gewährt.

Im Dezember 2004 (MasterCard) bzw. Februar 2005 (Visa) sind die bisher voneinander unabhängigen technischen Anforderungen der Zahlungssysteme zu dem sog. **Payment Card Industry (PCI) Data Security Standard** zusammengeführt worden.

Dieser setzt sich zusammen aus

- PCI Data Security Requirements, Version: January 2005, MasterCard Website
- PCI Self-Assessment Questionnaire, Version: January 2005 MasterCard Website
- PCI Security Scanning Procedures, Version: January 2005, MasterCard Website
- PCI Audit Procedures, Version: January 2005, MasterCard Website



und ist abrufbar unter

<https://sdp.mastercardintl.com/> bzw. <http://www.visaeurope.com/acceptingvisa/ais.html>.

Um den Nachweis der Umsetzung der Programme zu erbringen, sind seitens der Vertragsunternehmen folgende Schritte durchzuführen, in Abhängigkeit von deren Einstufung (s.u.):

- Der Händler nimmt eine erste Bewertung seiner Sicherheitsmaßnahmen anhand eines von SRC zu Verfügung gestellten Fragebogens (**Self-Assessment Questionnaire**) vor. Dieser Fragebogen muss jährlich neu ausgefüllt werden.
1. Es wird ein **Security Scan** der Internet-Schnittstelle des Händlers (sofern relevant) mit dem Ziel durchgeführt, ggf. vorhandene Schwachstellen aufzudecken, die durch Angreifer ausgenutzt werden könnten.
 2. Die Einhaltung der Sicherheitsanforderungen wird vor Ort mittels **Security Audit** geprüft.

Die folgende Tabelle gibt einen Überblick über die durchzuführenden Sicherheitsprüfungen in Abhängigkeit von der Anzahl der Transaktionen:

	Kategorie Händler	Self Assessment	Security Scan	Security Audit
	Level 1	-	4 x pro Jahr	1 x pro Jahr
	Level 2	1 x pro Jahr	4 x pro Jahr	-
	Level 3	1 x pro Jahr	4 x pro Jahr	-
	Level 4	1 x pro Jahr	1 x pro Jahr	-

Der Einstufung von Händlern gemäß MasterCard¹ und Visa² liegen folgende Kriterien zu Grunde:

- Level 1:
 - alle Händler, unabhängig vom Vertriebsweg (POS, MOTO oder E-Commerce), die mehr als 6 Millionen Transaktionen mit MasterCard oder Visa pro Jahr abwickeln;
 - alle Händler, die Opfer eines Angriffs und einer Kompromittierung geworden sind;
 - alle Händler, die mit einer anderen Kreditkartenmarke in die Kategorie Level 1 fallen;
 - alle Händler, die nach dem Ermessen von MasterCard oder Visa zur Minderung des Risikos für die Zahlungssysteme in diese Kategorie eingestuft werden.
- Level 2:
 - alle Händler, die zwischen 150.000 und 6 Millionen E-Commerce Transaktionen mit MasterCard- oder Visa-Karten abwickeln;
 - alle Händler, die mit einer anderen Kreditkartenmarke in die Kategorie Level 2 fallen.
- Level 3:
 - alle Händler, die zwischen 20.000 und 150.000 E-Commerce Transaktionen mit MasterCard- oder Visa-Karten abwickeln;
 - alle Händler, die mit einer anderen Kreditkartenmarke in die Kategorie Level 3 fallen.
- Level 4:
 - alle Händler, die nicht in eine der Kategorien Level 1, 2 oder 3 eingestuft sind.

¹ gemäß MasterCard Global Security Bulletin No. 1, 14 January 2005

² gemäß Visa Member Letter EU 06/05, 2 February 2005

MasterCard und Visa schreiben für Händler der Kategorien **Level 1 bis 3** die Erbringung des Nachweises über die Umsetzung der PCI Standards, Version 1.0, bis zum **30. Juni 2005** zwingend vor.

Für Händler der Kategorie **Level 4** wird eine Umsetzung der Programme dringend empfohlen.

Die Auswertung des Self-Assessments mittels Fragebogen, der Security Scan und der Security Audit werden durch von den Kreditkartenorganisationen akkreditierte Partner (Visa AIS Security Assessor bzw. MasterCard Security Vendor) durchgeführt.

SRC hat als weltweit erstes Unternehmen sowohl den Akkreditierungsprozess bei MasterCard als auch bei Visa erfolgreich abgeschlossen und unterstützt Acquirer bei der Umsetzung des MasterCard SDP- und Visa AIS-Programms.

Nachfolgend werden die Vorgehensweisen bei der Durchführung der einzelnen Schritte zum Nachweis der Konformität zu den Anforderungen von MasterCard und Visa erläutert.

2 Vorgehensweise und Ablauf

Der Internet-Händler hat von seinem Acquirer oder von SRC eine Mitteilung mit den Zugangs-Informationen zu der Web-Seite von SRC erhalten. Die Registrierung, die ca. 15 Minuten in Anspruch nimmt, ist **kostenlos** und wird durch ein Passwort und/oder einen Code geschützt, welches vom Acquirer oder von SRC mitgeteilt wird.

Im Rahmen der kostenlosen Registrierung müssen in einem Web-Formular verschiedene Fragen beantwortet werden, wie z. B.:

- Name der Firma, Adresse, Ansprechpartner und Kontaktdaten (E-Mail und Telefon);
- Anzahl der Transaktionen mit MasterCard-, Visa-, American Express-, Diners-, JCB- und Discovery-Kreditkarten;
- Angabe, ob Kreditkartendaten auf eigenen Systemen gespeichert, verarbeitet oder weitergeleitet werden;
- Nutzung eines Payment Service Providers und Name für die Abwicklung der Transaktionen;

Das Web-Formular muss vollständig und wahrheitsgemäß ausgefüllt werden; auf der Basis dieser Informationen werden anhand der o.g. Kriterien die nachfolgend durchzuführenden Schritte automatisch ermittelt.

Die ausgewerteten Informationen werden in einem weiteren Schritt in einem Registrierungsformular (PDF-Dokument) zusammengefasst. Dieses beinhaltet neben der Übersicht über die nachfolgend erforderlichen Schritte eine Aufstellung, mit der der Händler u. a. die einzelnen Leistungspakete bestellen (Fragebogen, Security Scan, Security Audit) kann. Dieses Registrierungsformular muss ausgedruckt und rechtsverbindlich unterzeichnet per Fax oder Brief an SRC übersendet werden.

Nachdem die Bestellung für die erforderlichen Leistungspakete bei SRC eingetroffen ist, wird der Händler für die Nutzung des Online-Fragebogens (Self-Assessment Questionnaire) freigeschaltet und per E-Mail informiert.

Der Termin und die weitere Vorgehensweise für den oder die erforderlichen Security Scans wird nachfolgend zwischen dem Händler und SRC vereinbart.

In den weiteren Abschnitten werden die Inhalte und Vorgehensweisen bei der Durchführung von Self-Assessment, Security Scan und Security Audit im Einzelnen erläutert.

3 Elektronischer Online-Fragebogen/PCI Self-Assessment Questionnaire

Ein Händler (Level 2-4) muss **jährlich** eine Bewertung der technischen und organisatorischen Maßnahmen durch Beantwortung des vorgegebenen PCI Self-Assessment Questionnaires (in deutsch/englisch) als Online-Fragebogen bei SRC durchführen.

Die Fragen betreffen sämtliche sechs Bereiche des PCI Data Security Standards und beinhalten zwölf Prüfungsanforderungen:

1. Aufbau und Instandhaltung des sicheren Netzwerks (Build and Maintain a Secure Network)
 - Anforderung 1: Einrichtung und Instandhaltung der Firewallkonfiguration zum Schutz der Daten
 - Anforderung 2: Keine Verwendung der vom Händler ausgelieferten voreingestellten System-Passwörter und anderer Sicherheitsparameter
2. Schutz der Karteninhaberdaten (Protect Cardholder Data)
 - Anforderung 3: Schutz der gespeicherten Daten
 - Anforderung 4: Verschlüsselte Übertragung der Karteninhaberdaten und sensiblen Informationen über öffentliche Netze
3. Aufrechterhaltung eines Programms zur Handhabung der Schwachstellen (Maintain a Vulnerability Management Program)
 - Anforderung 5: Gebrauch und regelmäßige Aktualisierung der Anti-Viren-Programme
 - Anforderung 6: Entwicklung und Aufrechterhaltung von sicheren Systemen und Anwendungen
4. Einführung von strengen Zugriffskontrolle-Maßnahmen (Implement Strong Access Control Measures)
 - Anforderung 7: Beschränkung des Zugriffs auf die Daten nach dem need-to-know Prinzip
 - Anforderung 8: Zuweisung von eindeutigen Kennungen an alle Personen mit Computer-Zugriff
 - Anforderung 9: Einschränkung des physischen Zugangs zu Karteninhaberdaten
5. Regelmäßige Überwachung und Untersuchung der Netzwerke (Regularly Monitor and Test Networks)
 - Anforderung 10: Verfolgung und Überwachung aller Zugriffe auf Netzwerk-Ressourcen sowie Karteninhaberdaten
 - Anforderung 11: Regelmäßige Prüfungen der Sicherheitssysteme und -prozesse
6. Aufrechterhaltung von Informationssicherheitspolitik (Maintain an Information Security Policy)
 - Anforderung 12: Aufrechterhaltung von Informationssicherheitspolitik

Mit dem Fragebogen wird die Einhaltung der Sicherheitsanforderungen des PCI Data Security Standards mittels Selbstauskunft geprüft.

Der Fragebogen muss nach der vollständigen Beantwortung aller Fragen ausgedruckt und rechtsverbindlich unterzeichnet per Fax oder Brief an SRC übersendet werden.

Im Zuge der automatischen Auswertung des Fragebogens werden die Antworten elektronisch zur Auswertung an SRC übermittelt und dort gespeichert.

Die Nutzung und automatisierte Auswertung des Fragebogens beinhaltet **eine halbe Stunde** Unterstützung per E-Mail, Telefon oder Fax bei der Beantwortung der Fragen.

Sollten sich Änderungen an den E-Commerce-Systemen ergeben, so ist der Internet-Händler gemäß der Regularien von MasterCard und Visa verpflichtet, den Fragebogen unverzüglich erneut zu beantworten, und sowohl in Papierform rechtsverbindlich unterzeichnet (per Fax oder Brief), als auch elektronisch an SRC zu übermitteln.

4 Security Scan

Security Scans haben das Ziel, Schwachstellen in Architektur und Konfiguration der untersuchten Systeme aufzudecken, die ein Angreifer ausnutzen könnte, um Kreditkartendaten zu kompromittieren.

SRC führt Security Scans entsprechend der Anforderungen aus den „PCI Security Scanning Procedures“³ durch. Diese werden als „**non-intrusive**“ bzw. „**non-destructive**“ durchgeführt, d.h. es werden keine Angriffe durchgeführt oder Schwachstellen ausgenutzt, die die Verfügbarkeit oder Integrität der Zielsysteme beeinflussen. Vielmehr werden reguläre Anfragen an die Zielsysteme gerichtet, die in der Regel keine Auswirkungen auf den ordnungsgemäßen Betrieb haben.

Die Systeme werden dabei aus dem Internet netzseitig mit Hilfe von Security Scannern und manueller Analysen auf mögliche Schwächen hin untersucht. Die eingesetzten Werkzeuge prüfen auf aktuell bekannte Schwächen von Netzwerkkomponenten, Betriebssystemen und Applikationen.

Der genaue Termin für die Durchführung der Security Scans wird zuvor mit dem Händler abgestimmt. Anschließend wird anhand einer einheitlichen und durch die „PCI Security Scanning Procedures“ vorgegebenen Vorgehensweise der Security Scan durchgeführt. Das Ergebnis des Security Scans wird in Form eines schriftlichen Berichts in **englischer** Sprache an den Internet-Händler übergeben. Der Bericht entspricht den Vorgaben von MasterCard und Visa und beinhaltet eine fünfstufige Kategorisierung (low, ..., urgent) der ggf. gefundenen Schwachstellen.

Die Untersuchung hat den Zweck, gezielt **einzelne** Schwachstellen oder Fehler aufzudecken, die zu Angriffen auf das System ausgenutzt werden können. Die funktionelle Korrektheit, das Leistungsverhalten der Implementierung und die generelle Freiheit von unerwünschten Schwachstellen oder Nebeneffekten werden nicht untersucht.

Sind aufgrund aufgedeckter Schwachstellen die Ergebnisse des Security Scans im Sinne der „PCI Security Scanning Procedures“ nicht zufriedenstellend, sind entsprechende Nachbesserungen durch den Händler erforderlich. Deren Wirksamkeit wird durch eine Wiederholung des Security Scans von SRC geprüft. Die Wiederholungsprüfung erfolgt **innerhalb von 10 Werktagen** in Abstimmung mit dem Händler. Sollte diese Frist nicht eingehalten werden, so wird SRC umgehend den zuständigen Acquirer in Kenntnis setzen, der dann ggf. weitere Schritte einleiten wird. Eine wiederholte Prüfung wird, ebenso wie Security Scans für zusätzliche IP-Adressen, gesondert in Rechnung gestellt.

SRC weist daraufhin, dass die Durchführung von Security Scans die Verfügbarkeit und Integrität der Zielsysteme beeinträchtigen kann. Es ist möglich, dass der ordnungsgemäße Betrieb nur durch einen manuellen Eingriff in das Zielsystem wiederhergestellt werden kann. Für mögliche Schäden, die bei der Durchführung von Security Scans entstehen, die von dem Auftraggeber schriftlich beauftragt wurden, übernimmt SRC keine Haftung.

Die Durchführung des Security Scans beinhaltet eine **halbe Stunde** Unterstützung per E-Mail, Telefon oder Fax zur Vorbereitung und abschließenden Erläuterung der Ergebnisse des Security Scans.

³ http://www.visaeurope.com/acceptingvisa/pdf/PCI_Security_Scan_Procedures_1_0.pdf oder https://sdp.mastercardintl.com/pdf/PCS_Manual.pdf

5 Durchführung des Security Audit

Im Rahmen des Security Audit werden bei Händlern der Kategorie Level 1 zusätzlich nachfolgend beschriebene Prüfungsschritte durchgeführt. Der genaue Ablauf dieser Prüfung ist im SRC-Dokument „Guideline for the preparation of the PCI security audit“ dargestellt. SRC wird dieses Dokument dem Händler unmittelbar nach Einordnung in die Kategorie Level 1 zur Verfügung stellen.

Die Anforderungen an das Security Audit sind im Dokument „PCI Security Audit Procedures“ beschrieben, welches über die o.a. Internet-Adressen verfügbar sind. Mit der Durchführung eines Security Audits prüft SRC die Umsetzung des PCI Data Security Standards vor Ort.

Zur **Vorbereitung** des PCI Security Audit sind folgende Schritte durchzuführen:

1. Formelle Beauftragung der Dienstleistung bei SRC und vorläufige Vereinbarung eines Termins für das Security Audit. Hierbei ist die von den Zahlungssystemen für die Durchführung der Auditierungsschritte (Security Scan und Security Audit) vorgegebene Frist von **60 Tagen** einzuhalten.
2. Auslieferung der Dokumente zur Durchführung des Security Audit:
SRC übersendet die „PCI Security Audit Procedures and Reporting“ und die „SRC Guideline for the preparation of the PCI security audit“ an den Kunden in elektronischer Form. Gleichzeitig stimmt SRC ein Passwort ab bzw. übermittelt SRC einen öffentlichen PGP-Schlüssel für die Absicherung der weiteren Kommunikation.
3. Der elektronische Online-Fragebogen (PCI Self-Assessment Questionnaire) wird freigeschaltet um dem Kunden die erste Bewertung seiner PCI-Compliance zu ermöglichen.

Die **Durchführung** des PCI Security Audit erfolgt in fünf voneinander abhängigen und aufeinander aufbauenden Schritten, die nachfolgend beschrieben werden.

Schritt 1: Bewertung der Dokumente

Die in der "SRC Guideline for the preparation of the PCI security audit" aufgeführten Informationen und Dokumente sind spätestens **zwei Wochen** vor dem abgestimmten Security Audit-Termin an SRC zu übermitteln. SRC wird diese inhaltlich überprüfen und im Falle von Unstimmigkeiten bzw. Unklarheiten mit dem Händler Rücksprache halten.

SRC weist daraufhin, dass die Durchführung eines Security Audit erst nach einer vollständigen und erfolgreich abgeschlossenen Prüfung der erforderlichen Dokumente möglich ist. Falls die notwendigen Informationen nicht rechtzeitig an SRC übergeben werden, kann ggf. eine Verschiebung des Security Audit erforderlich sein, wodurch zusätzliche Kosten entstehen können.

Schritt 2: Security Audit vor Ort (Ortsbegehung)

SRC wird im Rahmen des Security Audit die Angaben des Händlers, die dieser im Dokument "PCI Security Audit Procedures" schriftlich niederlegt, vor Ort stichprobenartig prüfen. Die Prüfung deckt die o.g. sechs Bereiche des PCI Data Security Standards ab und beinhaltet u.a.:

- Vorstellung des Geschäftsmodells,
- Ablauf einer Kreditkartentransaktionen innerhalb der IT-Systeme (Datenfluss),
- Interviews mit Mitarbeitern, insbesondere auch mit Personen, die
 - Sicherheitsfunktionen im Unternehmen wahrnehmen,
 - Zugriff auf Kreditkartendaten haben,
 - für die Wartung und den Betrieb von Systemen verantwortlich sind, auf denen Kreditkartendaten gespeichert, verarbeitet oder weitergeleitet werden
- Einsichtnahme in Logdateien der relevanten Anwendungen,
- Besichtigung der Räume, des Rechenzentrum, des Serverraum, usw.

Für den Fall, dass der Händler andere als in der Checkliste vorgegebene Sicherheitslösungen umgesetzt hat (so genannte Compensating Controls – Ersatzmaßnahmen), wird SRC diese überprüfen und im Hinblick auf die Angemessenheit und Umsetzung des PCI Data Security Standard bewerten.

Schritt 3: Berichtsentwurf

SRC erstellt einen ersten Entwurf des abschließenden Audit-Berichts auf Basis des Dokuments „PCI Security Audit Procedures“.

SRC wird den Audit-Bericht innerhalb von 5-10 Arbeitstagen nach der Ortsbegehung zur Prüfung und Kommentierung an den Händler übermitteln. Der Berichtsentwurf ist zur Wahrung der von den Zahlungssystemen vorgegebenen Fristen innerhalb von 5 Arbeitstagen an SRC zurückzusenden.

Schritt 4: Vor-Version des Reports

SRC arbeitet die Kommentare des Händlers nach Abstimmung in den Berichtsentwurf ein und übermittelt diesen an die Zahlungssysteme. Dieser wird von den Zahlungssystemen geprüft und ggf. kommentiert, und an SRC zurückgesendet.

Schritt 5: Endgültige Version des Reports

SRC wird abschließend die Kommentare der Zahlungssysteme in den Audit-Bericht einarbeiten und diesen anschließend an den Händler und die Zahlungssysteme weiterleiten.

6 Vergütung und Abrechnung

Die Vergütung der aufgeführten Leistungen erfolgt gemäß der zum Zeitpunkt der Leistungserbringung gültigen Preisliste von SRC. Die aktuell gültige Preisliste ist nach erfolgreicher Registrierung im OSSP-System im Bereich FAQ (Frequently Asked Questions) verfügbar.

Die Abrechnung erfolgt anteilig gemäß den jeweils im Abrechnungsmonat erbrachten Leistungen, bevorzugt über das Bankeinzugsverfahren.

Alle Rechnungsbeträge sind zahlbar netto innerhalb von 14 Tagen nach Rechnungsstellung.

7 Kontakt für Rückfragen

Mitarbeiter von SRC stehen registrierten und angemeldeten Internet-Händlern

- per E-Mail unter: sdpais@src-gmbh.de
- per Telefon unter: **+49-(0)228-2806-166**
- per Fax unter: **+49-(0)721-151408862**

an Werktagen (**Montag bis Freitag**) zwischen **9 und 17 Uhr** für Rückfragen zur Verfügung.

8 Über SRC ...

SRC Security Research & Consulting GmbH ist das gemeinsame Kompetenzzentrum und Beratungsunternehmen für sicherheitsrelevante Anwendungen und Technologien der vier kreditwirtschaftlichen Verlage Bank-Verlag (Köln), Deutscher Genossenschafts-Verlag (Wiesbaden), Deutscher Sparkassen Verlag (Stuttgart) und VÖB-ZVD Bank für Zahlungsverkehrsdienstleistungen (Bonn).

SRC unterstützt als unabhängiges Beratungsunternehmen seine Kunden in allen Fragen der IT-Sicherheit und konzipiert, spezifiziert, entwickelt, evaluiert und zertifiziert Sicherheitsanwendungen, insbesondere in den Bereichen elektronischer Zahlungsverkehr, Chipkarten, E- und M-Commerce, digitalen Signaturen oder Sicherheit von Computernetzwerken.

SRC ist beim Bundesamt für Sicherheit in der Informationstechnik (BSI) als Prüfstelle für die Evaluierung von Sicherheitskomponenten nach Common Criteria (ISO 15408) akkreditiert.

SRC ist als Sicherheitsgutachter vom Zentralen Kreditausschuss der Spitzenverbände der deutschen Kreditwirtschaft anerkannt. In dieser Funktion begutachtet SRC die Sicherheit von Komponenten und Systemen, die zum elektronischen Bezahlen eingesetzt werden.

Mitarbeiter von SRC sind vom Bundesamt für Sicherheit in der Informationstechnik (BSI) als IT-Grundschutz-Auditoren lizenziert.

Mitarbeiter von SRC sind als Auditoren für Informationssicherheits-Managementsysteme nach BS 7799/ISO 17799 zertifiziert.

SRC ist bei MasterCard als sog. 'Logical Security Auditor' für die Auditierung von Kreditkartenpersonalisierungsunternehmen akkreditiert.