

Odvětví platebních karet (PCI)

Standard bezpečnosti dat (DSS)  
  
Dotazník pro sebehodnocení P2PE  
a Osvědčení o shodě

Pouze obchodníci používající hardwarové platební terminály v PCI SSC schváleném P2PE řešení, kteří neukládají data držitelů karet

Pro užití s PCI DSS verze 3.2.1  
Revize 1.0.

Červen 2018

# Změny dokumentu

| **Datum** | **Verze** | **Revize SAQ** | **Popis** |
| --- | --- | --- | --- |
| N/A | 1.0 |  | Nepoužíváno. |
| Květen 2012 | 2.0 |  | Sjednocení obsahu dokumentu s požadavky nového Standardu bezpečnosti dat odvětví platebních karet v. 2.0 a testovacími postupy. |
| únor 2014 | 3.0 |  | Sjednocení obsahu dokumentu s požadavky nového Standardu bezpečnosti dat odvětví platebních karet v. 3.0, testovacími postupy a zahrnutí další možnosti odpovědi. |
| duben 2015 | 3.1 |  | Aktualizace dokumentu za účelem sjednocení s verzí PCI DSS 3.1. Detaily změn PCI DSS jsou k dispozici v dokumentu Summary of Changes from PCI DSS Version 3.0 to 3.1 (PCI DSS – Seznam změn PCI DSS verze 3.0 do 3.1).  Odstraněno „HW“ z názvu SAQ, protože může být používán obchodníky používající HW/HW nebo HW/Hybridní P2PE řešení. |
| červenec 2015 | 3.1 | 1.1 | Aktualizace za účelem odstranění odkazů na „osvědčené postupy“ před 30. červnem 2015 a odstranění možnosti v2 pro požadavek 11.3 |
| duben 2016 | 3.2 | 1.0 | Aktualizace dokumentu za účelem sjednocení s verzí PCI DSS v3.2. Detaily změn PCI DSS jsou k dispozici v dokumentu Summary of Changes from PCI DSS Version 3.1 to 3.2. (PCI DSS – Seznam změn PCI DSS verze 3.1 do 3.2).  Odstraněny PCI DSS požadavky 3.3 a 4.2, jak je popsáno v implementaci PCU P2PE řešení a PIM. |
| leden 2017 | 3.2 | 1.1 | Aktualizace změn dokumentu, aby vysvětlovaly odstranění požadavků v aktualizaci duben 2016. |
| červen 2018 | 3.2.1 | 1.0 | Aktualizace dokumentu za účelem sjednocení s verzí PCI DSS v3.2.1. Detaily změn PCI DSS jsou k dispozici v dokumentu Summary of Changes from PCI DSS Version 3.2 to 3.2.1 (PCI DSS – Seznam změn PCI DSS verze 3.2 do 3.2.1). |

# Obsah

[Změny dokumentu 1](#_Toc13820422)

[Obsah 2](#_Toc13820423)

[Než začnete 3](#_Toc13820424)

[PCI DSS – Postup vyplnění sebehodnotícího dotazníku 3](#_Toc13820425)

[Jak porozumět sebehodnotícímu dotazníku 3](#_Toc13820426)

[Očekávané testování 4](#_Toc13820427)

[Vyplnění sebehodnotícího dotazníku 5](#_Toc13820428)

[Postup v případech, kdy nelze aplikovat dané požadavky 5](#_Toc13820429)

[Výjimky ze zákona 5](#_Toc13820430)

[Oddíl 1: Informace o hodnocení 6](#_Toc13820431)

[Oddíl 2: Dotazník pro sebehodnocení P2PE 9](#_Toc13820432)

[Ochrana dat držitelů karet 9](#_Toc13820433)

[Požadavek 3: Chránit uchovávaná data držitelů karet 9](#_Toc13820434)

[Požadavek 9: Omezit fyzický přístup k datům držitelů karet 11](#_Toc13820435)

[Udržování politiky bezpečnosti informací 14](#_Toc13820436)

[Požadavek 12: Udržovat politiku zaměřenou na informační bezpečnost pro všechen personál 14](#_Toc13820437)

[Příloha A1: Dodatečné požadavky PCI DSS na poskytovatele sdíleného hostingu 16](#_Toc13820438)

[Příloha A2: Dodatečné požadavky na subjekty používající SSL/dříve TLS pro transakce za fyzické přítomnosti platební karty u POS POI terminálových připojení 16](#_Toc13820439)

[Příloha A3: Dodatečné hodnocení pro specifické subjekty DESV (Designated Entities Supplemental Validation) 16](#_Toc13820440)

[Příloha B: Pracovní list náhradního řešení 17](#_Toc13820441)

[Příloha C: Vysvětlení pro „Nevztahuje se”(N/A) 18](#_Toc13820442)

[Oddíl 3: Validace a podrobnosti o osvědčení 19](#_Toc13820443)

# Než začnete

SAQ P2PE byl vypracován tak, aby zohlednil požadavky vztahující se na obchodníky, kteří zpracovávají data držitelů karet pouze skrze hardwarové platební terminály zahrnuté ve validovaném a evidovaném PCI P2PE řešením.

SAQ P2PE obchodníci nemají přístup to dat držitelů karet na jakémkoliv počítačovém systému a pouze zadávají čísla karet skrze hardware platební terminál z PCI SSC schváleném řešení. SAQ P2PE obchodníci mohou být jak  v „kamenných obchodech“ (karta přítomna) tak přijímající písemné/telefonické objednávky (karta nepřítomna). Např. obchodník přijímající písemné/telefonické objednávky může být způsobilý k SAQ P2PE pokud přijímají data držitelů karet v papírové formě nebo přes telefon a zadají ho přímo a pouze do validovaného P2PE hardware zařízení.

SAQ P2PE potvrzují, že pro tento platební kanál:

* Veškeré zpracování plateb je validován skrze PCI P2PE řešení schváleným a evidovaným PCI SSC.
* Jediná zařízení v obchodníkově prostředí, které uchovávají, zpracovávají nebo přenáší čísla karet jsou POI zařízení, která jsou schválená pro použití s validovaným a evidovaným PCI P2PE řešením.
* Obchodník jinak nepřijímá nebo nepřenáší data držitelů karet.
* Obchodník potvrzuje, že nemá žádná zastaralá úložiště (legacy storage) dat držitelů karet ve svém prostředí.
* Obchodník uchovává pouze papírové záznamy nebo účtenky s jakýmikoliv daty držitelů karet a tyto dokumenty nejsou přijímány elektronicky.
* Obchodník implementoval všechny kontroly řízení z P2PE instrukčního manuálu (PIM) poskytnutého poskytovatelem P2PE řešení.

***Tento SAQ se nevztahuje na e-commerce kanály.***

Tato zkrácená verze SAQ obsahuje otázky vztahující se na specifický typ prostředí drobného obchodníka, jak je definováno ve výše uvedených kritériích způsobilosti. Pokud existují požadavky PCI DSS aplikovatelné na vaše prostředí, které nejsou pokryté tímto SAQ, může to být známkou toho, že tento SAQ není vhodný pro vaše prostředí. Navíc, musíte stále být v souladu se všemi aplikovatelnými požadavky PCI DSS, abyste byli v souladu s PCI DSS.

## PCI DSS – Postup vyplnění sebehodnotícího dotazníku

1. Nalezněte příslušný SAQ pro vaše prostředí – více naleznete v dokumentu Návody a pokyny k dotazníku pro vlastní hodnocení (*Self-Assessment Questionnaire Instructions and Guidelines)* na webových stránkách PCI SSC.
2. Potvrďte, že vaše prostředí je správně definováno a splňuje kritéria způsobilosti pro SAQ, který je použit (tak, jak je definováno v Části 2g Osvědčení o shodě).
3. Potvrďte, že jste implementoval všechny prvky PIM.
4. Posuďte, zda je vaše prostředí v souladu s příslušnými požadavky PCI DSS.
5. Vyplňte všechny části tohoto dokumentu:

* Oddíl 1 (Část 1 & 2 AOC) – Informace o hodnocení a Shrnutí.
* Oddíl 2 – PCI DSS sebehodnotící dotazník (SAQ P2PE)
* Oddíl 3 (Část 3 & 4 AOC) – validace a podrobnosti o osvědčení, akční plán pro ty požadavky, které nebyly splněny (v případě potřeby)

1. Předložte Dotazník SAQ a Osvědčení o shodě AOC (Attestation of Compliance) spolu s další požadovanou dokumentací, své acquirerské bance, kartovým asociacím nebo dalším žadatelům.

## Jak porozumět sebehodnotícímu dotazníku

Otázky obsažené ve sloupci „PCI DSS Otázka“ v tomto sebehodnotícím dotazníku jsou založeny na požadavcích PCI DSS.

Na pomoc s procesem hodnocení slouží další zdroje, které poskytují návod k PCI DSS požadavkům a k vyplnění sebehodnotícího dotazníku. Přehled některých zdrojů je uveden níže:

|  |  |
| --- | --- |
| **Dokument** | **Zahrnuje:** |
| PCI DSS  Požadavky a postupy posouzení bezpečnosti Standardu bezpečnosti dat v odvětví platebních karet  *(PCI Data Security Standard Requirements and Security Assessment Procedures* | * Návod pro stanovení rozsahu * Pokyny k záměru všech PCI DSS požadavků * Podrobnosti testovacích postupů * Pokyny týkající se Náhradních řešení |
| Návody a pokyny k dotazníku pro sebehodnocení SAQ  *(Self-Assessment Questionnaire Guidelines and Instructions)* | * Informace o všech SAQ a jejich kritériích způsobilosti * Jak určit, který SAQ je správný pro vaši společnost |
| Slovník pojmů, zkratek a akronymů PCI DSS a PCI PA-DSS  *(PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms)* | * Popis a definice pojmů používaných v PCI DSS a v sebehodnotících dotaznících |

Tyto a další zdroje jsou k naleznutí na webových stránkách PCI SSC ([www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)). Společnosti jsou nabádány, aby prozkoumaly PCI DSS a další podpůrné dokumenty před začátkem vlastního hodnocení.

### Očekávané testování

Instrukce, které jsou poskytnuté ve sloupci „Očekávané testování“, jsou založeny na testovacích postupech v PCI DSS a obsahují tzv. high-level popis testovacích postupů, které by měly být vykonány za účelem ověření, zda byl konkrétní požadavek splněn. Plné znění testovacích postupů pro každý požadavek je k naleznutí v PCI DSS.

## Vyplnění sebehodnotícího dotazníku

Pro každou otázku existuje výběr odpovědí naznačující stav Vaší společnosti týkající se daného požadavku. ***Může být vybrána pouze jedna odpověď pro každou otázku***.

Popis významu každé odpovědi je poskytnut v této tabulce:

| **Odpověď** | **Popis** |
| --- | --- |
| **Ano** | Očekávané testování bylo provedeno a všechny části požadavku byly splněny. |
| **Ano s CCW** (Pracovní tabulka náhradního řešení) | Očekávané testování bylo provedeno a všechny části požadavků byly splněny s pomocí náhradního řešení.  Všechny odpovědi v tomto sloupci je zapotřebí vyplnit v Pracovní tabulce náhradního řešení (CCW) v příloze B dotazníku (SAQ).  Informace o využití náhradního řešení a návod, jak vyplnit pracovní list, jsou poskytnuty v PCI DSS. |
| **Ne** | Některé nebo žádné části požadavku nebyly splněny nebo jsou v procesu implementace nebo vyžadují další testování předtím, než bude známo, jestli jsou již implementovány. |
| **N/A**  (“Nevztahuje se“) | Požadavky, které se nevztahují na vaše prostředí. (Více k nalezení v: *„Guidance for Non-Applicability of Certain, specific Requirements below for examples“)*  Všechny odpovědi v tomto sloupci vyžadují další vysvětlení v příloze C dotazníku SAQ. |

## Postup v případech, kdy nelze aplikovat dané požadavky

V případě, že některý z požadavků nelze aplikovat na vaše prostředí, vyberte u daného požadavku možnosti „N/A“ a vyplňte „Explanation of Non-Applicability“ (Vysvětlení pro „Nevztahuje se“) v odpovídající části formuláře Přílohy C.

## Výjimky ze zákona

V případě, že vaše společnost podléhá právním omezením, které znemožňují dodržování požadavků PCI DSS, uveďte u daného požadavku „No“ a vyplňte odpovídající osvědčení v Části 3.

# Oddíl 1: Informace o hodnocení

***Pokyny pro předložení***

Tento dokument musí být vyplněn jako deklarace výsledků sebehodnocení obchodníka podle *Požadavků a postupů posouzení bezpečnosti Standardu bezpečnosti dat v odvětví platebních karet (PCI DSS)*. Vyplňte všechny části: Poskytovatel služeb je odpovědný za to, aby každá část byla vyplněna relevantními stranami. Kontaktujte odpovídající kartovou společnost, aby stanovila reporting a způsob předložení.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Část 1. Informace o poskytovateli služeb a společnosti kvalifikovaných hodnotitelů bezpečnosti** | | | | | | | |
| **Část 1a. Informace o poskytovateli služeb** | | | | | | | |
| Název společnosti: |  | | Obch. jméno: | |  | | |
| Kontaktní jméno: |  | | Funkce: | |  | | |
| Telefon: |  | | E-mail: | |  | | |
| Sídlo společnosti: |  | | Město: | |  | | |
| Stát / kraj: |  | Země: |  | | | PSČ: |  |
| URL: |  | | | | | | |
| **Část 1b. Informace o společnosti kvalifikovaných hodnotitelů bezpečnosti QSA (lze-li aplikovat)** | | | | | | | |
| Název společnosti: |  | | | | | | |
| Kontaktní jméno hlavního hodnotitele: |  | | Funkce: |  | | | |
| Telefon: |  | | E-mail: |  | | | |
| Sídlo společnosti: |  | | Město: |  | | | |
| Stát / kraj: |  | Země |  | | | PSČ: |  |
| URL: |  | | | | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | **Část 2. Shrnutí:** | | | | **Část 2a. Druh podnikání obchodníka (zatrhněte vše, co lze aplikovat):** | | | | Maloobchod  Telekomunikace  Obchody a supermarkety | | | | Pohonné hmoty  E-Commerce  Písemné / telefonické objednávky (MOTO) | | | | Jiné (specifikujte): | | | | Který typ/typy platebních kanálů je/jsou využívány ve Vašem podnikání?  Písemná / telefonická objednávka (MOTO)  E-Commerce  Přítomnost platební karty (face-to-face) | | Na které typy platebních kanálů se vztahuje tento dotazník SAQ?  Písemná / telefonická objednávka (MOTO)  E-Commerce  Přítomnost platební karty (face-to-face) | | ***Poznámka:*** *Využívá-li vaše organizace platební kanál či proces, na který se nevztahuje tento dotazník SAQ, zkonzultujte se svou acquirerskou bankou nebo kartovou asociací ověření pro ostatní kanály.* | | | |  | | | | **Část 2b. Popis typu podnikání s ohledem na platební karty** | | | | Jak a v jakém množství při Vašem podnikání uchováváte, zpracováváte a/nebo přenášíte data držitelů karet? |  | | | | |
| **Část 2c. Lokace (umístění)** | | |
| Seznam všech typů zařízení (např. prodejny, firemní kanceláře, datová centra, call centra atd.) a shrnutí všech lokací zahrnutých v PCI DSS posudku. | | |
| **Druh zařízení** | **Počet zařízení tohoto typu** | **Umístění zařízení (město, země)** |
| Příklad: maloobchodní prodejny | 3 | Boston, MA, USA |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |
| --- | --- |
| **Část 2d. Platební aplikace** | |
| Poskytněte následující informace týkající se validovaného PCI P2PE řešení, které vaše společnost používá: | |
| **Název poskytovatele P2PE řešení:** |  |
| **Název P2PE řešení:** |  |
| **PCI SSC referenční číslo:** |  |
| **P2PE POI zařízení používané Obchodníkem** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Část 2e. Popis prostředí** | | | |
| Poskytněte „**high-level**“ popis vašeho prostředí, na které se vztahuje toto hodnocení.  *Například:*   * *Spojení do a z prostředí dat držitelů karet (CDE)* * *Kritické komponenty systému v rámci CDE, jako například POS zařízení, databáze, webový server atd., a další nezbytné komponenty, podle potřeby.* |  | | |
| Používá Vaše společnost síťovou segmentaci za účelem ovlivnění rozsahu prostředí PCI DSS?  *(Viz. Pokyny týkající se části „Síťová segmentace“ v PCI DSS)* | | Ano  Ne | |
| |  |  |  | | --- | --- | --- | | **Část 2f. Poskytovatelé služeb – třetí strany** | | | | Používá Vaše společnost kvalifikovaného integrátora či prodejce (QIR)? | | Ano  Ne | | **V případě, že Ano:** | | | | **Jméno QIR společnosti:** |  | | | **Jméno zástupce QIR společnosti:** |  | | | **Popis poskytovaných služeb:** |  | | | | |
| Sdílí Vaše společnost kartová data s třetími stranami – poskytovateli služeb (např. kvalifikovaní integrátoři a prodejci (QIR), platební brány, zpracovatelé plateb, poskytovatelé platebních služeb (PSP), poskytovatelé webového hostingu, agentury poskytující letecké rezervace, společnosti zabývající se věrnostním programem apod.)? | | Ano  Ne |

|  |  |
| --- | --- |
| **V případě, že Ano:** | |
| **Jméno poskytovatele služeb:** | **Popis poskytovaných služeb:** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| ***Poznámka:*** *Požadavek 12.8 se vztahuje na všechny subjekty v tomto seznamu.* | |

|  |
| --- |
| **Část 2g. Způsobilost k vyplnění SAQ P2PE** |

|  |  |
| --- | --- |
| Obchodník potvrzuje, že je způsobilý k vyplnění této zkrácené verze Dotazníku pro sebehodnocení, protože pro tento platební kanál: | |
|  | Veškeré zpracování plateb je validován skrze PCI P2PE řešení schváleným a evidovaným PCI SSC. |
|  | Jediná zařízení v obchodníkově prostředí, které uchovávají, zpracovávají nebo přenáší čísla karet jsou POI zařízení, která jsou schválená pro použití s validovaným a evidovaným PCI P2PE řešením. |
|  | Obchodník jinak nepřijímá nebo nepřenáší data držitelů karet. |
|  | Obchodník potvrzuje, že nemá žádná zastaralá úložiště (legacy storage) dat držitelů karet ve svém prostředí. |
|  | Obchodník uchovává pouze papírové záznamy nebo účtenky s jakýmikoliv daty držitelů karet a tyto dokumenty nejsou přijímány elektronicky. |
|  | Obchodník implementoval všechny kontroly řízení z P2PE instrukčního manuálu (PIM) poskytnutého poskytovatelem P2PE řešení. |

# Oddíl 2: Dotazník pro sebehodnocení P2PE

|  |
| --- |
| ***Poznámka:*** *Následující otázky jsou očíslovány podle Požadavků a testovacích postupů PCI DSS, jak jsou definovány v dokumentu Požadavky a postupy posouzení bezpečnosti Standardu bezpečnosti dat v odvětví platebních karet.* |

**Datum vyplnění:**

## Ochrana dat držitelů karet

### Požadavek 3: Chránit uchovávaná data držitelů karet

***Poznámka:*** *Požadavek 3 se vztahuje pouze na SAQ P2PE obchodníky, kteří mají papírové záznamy (například, účtenky, tištěné záznamy, atd.) s čísly karet včetně primárních čísel účtů (PAN).*

| **PCI DSS Otázka** | | **Očekávané Testování** | **Odpověď**  **(zaškrtněte jednu odpověď pro každou otázku)** | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **ANO** | **ANO s „CCW“** | **NE** | **N/A** | |
| 3.1 | Jsou politiky, postupy a procesy držení a mazání dat implementovány dle následujícího: |  | | | | |
| (a) Je množství dat a doba jejich držení omezeno na nezbytně nutné z právních, regulačních a/nebo provozních důvodů? | * Zkontrolujte politiky a postupy pro držení a likvidaci dat * Rozhovor s personálem |  |  |  |  | |
| (b) Jsou definovány procesy bezpečného mazání dat držitelů karet, jakmile nejsou zapotřebí z právních, regulačních a/nebo provozních důvodů? | * Zkontrolujte politiky a postupy * Rozhovor s personálem * Přezkoumejte mechanismus mazání |  |  |  |  | |
| (c) Existují specifické požadavky na držení dat držitelů karet?  *Například data držitelů karet mají být uchovávána po X období z Y provozních důvodů* | * Zkontrolujte politiky a postupy * Rozhovor s personálem * Přezkoumejte požadavky na držení dat |  |  |  |  | |
| (d) Je aplikován čtvrtletní proces na identifikování a bezpečné mazání uchovávaných dat držitelů karet, které přesahují definované požadavky na držení dat? | * Zkontrolujte politiky a postupy * Rozhovor s personálem * Sledujte procesy mazání |  |  |  |  | |
| (e) Splňují všechna uložená data držitelů karet požadavky definované politikou držení dat?? | * Přezkoumejte soubory a systémové záznamy |  |  |  |  | |
| ***Pokyny:*** *Odpověď „Ano“ na požadavek v 3.1 znamená, že pokud obchodník uchovává papírové záznamy (například účtenky nebo papírové záznamy), které obsahují čísla karet, obchodník uchovává takový záznam jen tak dlouho jak ho potřebuje pro účely podnikání nebo ze zákonných a regulatorních důvodů a zničí každý takový záznam, pokud ho již nadále není potřebný.*  *Pokud obchodník nikdy netiskne nebo neuchovává žádné papírové záznamy s čísly karet, měl by obchodník zaškrtnout „N/A“ sloupec a vyplnit Přílohu C „Vysvětlení pro Nevztahuje se”.* | | | | | | | |
| 3.2.2 | Není po autorizaci uchováván ověřovací kód/hodnota card verification code/value) (trojmístné nebo čtyřmístné číslo na líci nebo rubu platební karty) používané k verifikaci transakcí bez přítomnosti karty? | * Přezkoumejte zdroje dat včetně: * Příchozích transakčních dat * Všech záznamů * Historie souborů * Souborů trasování * Databázových schémat * Obsahů databází |  |  |  |  | |
| ***Pokyny:*** *Odpověď „Ano“ na požadavek v 3.2.2 znamená, že pokud obchodník zaznamenává bezpečnostní kód karty při provádění transakcí, obchodník buď bezpečně záznam zničí (např. skartovačkou) okamžitě po skončení transakce, nebo kód znehodnotí (např. začerní fixou) než bude záznam uložen.*  *Pokud obchodník nikdy neuchovává žádné záznamy s čísly karet, měl by obchodník zaškrtnout „N/A“ sloupec a vyplnit Přílohu C Vysvětlení pro „Nevztahuje se”* | | | | | | | |
| 3.7 | Jsou bezpečnostní politiky a provozní postupy pro ochranu uložených dat držitelů karet:   * dokumentovány, * používají se * jsou známy všem dotčeným stranám? | * Zkontrolujte bezpečnostní politiky a provozní postupy * Rozhovor s personálem |  |  |  |  | |
| ***Pokyny:*** *Odpověď „Ano“ na požadavek v 3.7 znamená, že pokud obchodník uchovává papírové záznamy s čísly karet, má obchodník zavedené politiky a postupy pro požadavky 3.1, 3.2.2 a 3.3. Toto pomáhá zajistit, že si je personál vědom a dodržuje bezpečnostní politiky a dokumentované provozní postupy pro bezpečné uchovávání dat držitelů karet na kontinuální bázi.* | | | | | | | |

### Požadavek 9: Omezit fyzický přístup k datům držitelů karet

***Poznámka:*** *požadavky 9.5 a 9.8 se vztahují pouze na SAQ P2PE obchodníky s papírovými záznamy (např. účtenky a papírové záznamy) s čísly karet, včetně primárních čísel účtů (PAN).*

| **PCI DSS Otázka** | | **Očekávané Testování** | **Odpověď**  **(zaškrtněte jednu odpověď pro každou otázku)** | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ANO** | **ANO s „CCW“** | **NE** | **N/A** |
| 9.5 | Jsou všechna média fyzicky zabezpečena (kromě jiných i u počítačů, vyjímatelných elektronických médií, papírových stvrzenek, papírových sestav a faxů)?  *Pro účely požadavku č. 9 „média“ jsou všechna papírová a elektronická média obsahující data držitelů karet* | * Zkontrolujte politiky a postupy pro fyzického zabezpečení medií * Rozhovor s personálem |  |  |  |  |
| 9.8 | (a) Jsou všechna média zničena, když jich již není zapotřebí z provozních ani právních důvodů? | * Zkontrolujte politiky a postupy periodické likvidace médií |  |  |  |  |
|  | (c) Jsou média zničena dle následujícího: |  | | | | | |
| 9.8.1 | (a) Jsou materiály s fyzickými kopiemi rozřezány, spáleny nebo rozdrceny tak, aby data držitelů karet nemohla být zrekonstruována? | * Rozhovor s personálem * Přezkoumejte postupy * Sledujte procesy |  |  |  |  |
| (b) Jsou skladovací kontejnery používané pro materiály, které obsahují informace určené ke zničení, zabezpečeny proti přístupu k jejich obsahu? | * Přezkoumejte bezpečnost skladovacích kontejnerů |  |  |  |  |
| ***Pokyny:*** *Odpověď „Ano“ na požadavky v 9.5 a 9.8 znamená, že obchodník bezpečně uchovává jakýkoliv záznam s čísly karet, např. uchovává je v zamčeném šuplíku, skříni nebo sejfu, a že obchodník zničí každý takový záznam, když již není nadále potřebný k účelu podnikání. Toto zahrnuje i psaný dokument nebo politiku pro zaměstnance, tak aby věděli, jak zabezpečit záznam s čísly karet a jak takový záznam zničit, když již není potřebný.*  *Pokud obchodník nikdy neuchovává žádné záznamy s čísly karet, měl by obchodník zaškrtnout „N/A“ sloupec a vyplnit Přílohu C „Vysvětlení pro Nevztahuje se”* | | | | | | | |
| 9.9 | Jsou chráněna zařízení, která získávají data platebních karet prostřednictvím přímé fyzické interakce s kartou, před nedovolenou manipulací a záměně dle následujícího?  ***Poznámka****: Tyto požadavky se vztahují na čtecí zařízení karet používaných při transakcích za přítomnosti karet (to znamená, že karta je protažena nebo vložena) v místě prodeje. Tento požadavek se nevztahuje na komponenty s ručním vstupem jako jsou počítačové klávesnice a POS klávesnice.* |  | | | | | |
| (a) Vyžadují politiky a postupy, aby byl seznam takových zařízení udržován? | * Zkontrolujte politiky a postupy |  |  |  |  |
| (b) Vyžadují politiky a postupy, aby byla prováděna pravidelná kontrola zařízení za účelem zjištění, zda s ním nebylo manipulováno nebo nebylo nahrazeno? | * Zkontrolujte politiky a postupy |  |  |  |  |
| (c) Vyžadují politiky a postupy školení personálu, aby si byli vědomi podezřelého chování a hlásili manipulaci nebo náhradu zařízení? | * Zkontrolujte politiky a postupy |  |  |  |  |  | | |
| 9.9.1 | (a) Obsahuje seznam zařízení následující body?   * Značku a model zařízení * Umístění zařízení (např. adresa místa nebo objektu, kde se zařízení nachází) * Sériové číslo zařízení nebo jiný způsob unikátní identifikace | * Přezkoumejte seznam zařízení |  |  |  |  |  | | |
|  | (b) Je seznam přesný a aktuální? | * Sledujte zařízení a jejich umístění a porovnejte se seznamem |  |  |  |  |  | | |
|  | (c) Je seznam zařízení aktualizován když je zařízení přidáno, přemístěno, vyřazeno z provozu atd.? | * Rozhovor s personálem |  |  |  |  |  | | |
| 9.9.2 | (a) Jsou pravidelně kontrolovány povrchy zařízení, aby se zjistila neoprávněná manipulace (např. přidání Skimmeru -nelegální čtečky karet do zařízen) nebo výměně (např. kontrolou sériového čísla nebo jiné charakteristiky zařízení pro ověření, zda zařízení nebylo vyměněno za podvodné) podle následujícího?  ***Poznámka****: Příklady příznaků, které naznačují, že se zařízením mohlo být manipulováno nebo bylo nahrazeno, jsou neočekávané přílepky nebo kabely zapojené do zařízení, chybějící nebo změněné bezpečnostní štítky, rozbité nebo jinak barevné kryty nebo změny sériového čísla nebo jiné vnější znaky.* | * Rozhovor s personálem * Sledujte procesy inspekce a porovnejte s definovanými procesy |  |  |  |  |  | | |
| (b) Je si personál vědom postupů pro prohlídky zařízení? | * Rozhovor s personálem |  |  |  |  |  | | |
| 9.9.3 | Je personál školen, aby si byl vědom pokusů o manipulaci se zařízením nebo jejich výměně, dle následujícího? |  | | | | | |
|  | (a) Obsahují školící materiály pro personál v místě prodeje následující?   * Ověřit identitu jakýchkoli osob třetí strany, které tvrdí, že je personál opravy nebo údržby, před udělením přístupu k provedení opravy nebo údržby zařízení. * Neinstalovat, nevyměňovat ani nevracet zařízení bez ověření. * Být si vědom podezřelého chování kolem zařízení (např. pokusy neznámých osob o odpojení nebo otevření zařízení). * Hlásit podezřelé chování a známky manipulace se zařízením nebo jeho výměnu (substituci) příslušnému personálu (například manažerovi nebo bezpečnostnímu pracovníkovi). | * Zkontrolujte školící materiály |  |  |  |  |  | | |
|  | (b) Je personál v místě prodeje školen a je si vědom postupů pro detekci a hlášení pokusů o manipulaci nebo výměnu zařízení? | * Rozhovor s personálem v umístění POS zařízení |  |  |  |  |  | | |
| ***Pokyny:*** *Odpověď „Ano“ na požadavek v 9.9 znamená, že obchodník má zavedené politiky a postupy k požadavkům 9.9.1-9.9.3. a že udržuje aktuální seznam zařízení, provádí pravidelné kontroly zařízení a školí své zaměstnance tak, aby byli schopni rozpoznat zařízení, se kterými bylo manipulováno nebo která byla zaměněna.* | | | | | | | |
| 9.10 | Jsou bezpečnostní politiky a provozní postupy pro omezení fyzického přístupu k datům držitelů karet:   * dokumentovány * používají se * jsou známy všem dotčeným stranám? | * Přezkoumejte bezpečnostní politiky a provozní postupy * Rozhovor s personálem |  |  |  |  |  | | |
| ***Pokyny:*** *Odpověď „Ano“ na požadavek v 9.10 znamená, že obchodník má zavedené politiky a postupy k požadavkům 9.5, 9.8 a 9.9, příslušně svému prostředí. Toto pomáhá zajistit, že si je personál vědom a dodržuje bezpečnostní politiky a dokumentované provozní postupy.* | | | | | | | |

## Udržování politiky bezpečnosti informací

### Požadavek 12: Udržovat politiku zaměřenou na informační bezpečnost pro všechen personál

***Poznámka:*** *Požadavek 12 specifikuje, že obchodník musí mít nastaveny informačně bezpečnostní politiky pro své zaměstnance, nicméně tyto politiky mohou být tak jednoduché nebo složité, jak je potřeba, dle velikosti a komplexnosti obchodníkových činností. Takovýto dokument musí být poskytnut všem zaměstnancům tak, aby si byli vědomi své odpovědnosti za ochranu platebních terminálů, dokumentů s daty držitelů karet atd. Pokud nemá obchodník žádné zaměstnance očekává se, že si je obchodník vědom a chápe svou odpovědnost za bezpečnost ve svých obchodech.*

| **PCI DSS Otázka** | | **Očekávané Testování** | **Odpověď**  **(zaškrtněte jednu odpověď pro každou otázku)** | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ANO** | **ANO s „CCW“** | **NE** | **N/A** | |
| 12.1 | Je bezpečnostní politika zavedena, zveřejněna, udržována a rozšířena veškerému příslušnému personálu? | * Zkontrolujte politiku informační bezpečnosti |  |  |  |  | |
| 12.1.1 | Je bezpečnostní politika zkontrolována nejméně jednou ročně a aktualizována pokaždé změně prostředí? | * Zkontrolujte politiku informační bezpečnosti * Rozhovor s odpovědným personálem |  |  |  |  | |
| ***Pokyny:*** *Odpověď „Ano“ na požadavek v 12.1 znamená, že obchodník má bezpečnostní politiku, smysluplnou vzhledem k velikosti a komplexitě obchodníkových činností, a tato politika je ročně vyhodnocována a aktualizována, pokud je třeba. Např. takováto politika může být jednoduchý dokument, který pokrývá jak chránit obchod a platební zařízení v souladu s P2PE instrukčním manuálem (PIM) a kam zavolat v případě nouze.* | | | | | | |
| 12.4 | Definuje jasně bezpečnostní politika a postupy odpovědnost v oblasti informační bezpečnosti pro všechen personál? | * Zkontrolujte politiku a postupy informační bezpečnosti * Rozhovor se vzorkem odpovědného personálu |  |  |  |  | |
| ***Pokyny:*** *Odpověď „Ano“ na požadavek v 12.4 znamená, že obchodníkova bezpečnostní politika definuje základní bezpečnostní odpovědnost pro všechen personál, konzistentní s velikostí a komplexností obchodníkových činností. Např. bezpečnostní odpovědnost může být definována podle základních odpovědností dle pozic zaměstnanců, jako jsou odpovědnosti očekávané od manažera, vlastníka a ty očekávané od prodavačů.* | | | | | | |
| 12.5 | Jsou následující odpovědnosti bezpečnosti informací specificky a formálně přiděleny jedinci nebo týmu: |  | | | | |
| 12.5.3 | Vytváření, dokumentování a distribuce reakcí na bezpečnostní incidenty a eskalačních postupů k zajištění včasného a efektivního nakládání s nimi za všech situací? | * Zkontrolujte politiky a postupy informační bezpečnosti |  |  |  |  | |
| ***Pokyny:*** *Odpověď „Ano“ na požadavek v 12.5.3 znamená, že má obchodník určenou osobu, která je odpovědná za reakce na incident a jeho eskalaci požadovaný v 12.9.* | | | | | | | |
| 12.6 | (a) Existuje a poskytuje formální program bezpečnostního povědomí celému personálu informace o politikách a postupech bezpečnosti dat držitelů karet? | * Zkontrolujte program povědomí o bezpečnosti |  |  |  |  | |
| ***Pokyny:*** *Odpověď „Ano“ na požadavek v 12.6. znamená, že obchodník má nastavený program bezpečnostního povědomí, konzistentní s velikostí a komplexností obchodníkových činností. Např. jednoduchý plán povědomí může být leták vyvěšený v backoffice nebo email periodicky zasílaný všem zaměstnancům. Příklady obsahu zprávy bezpečnostního povědomí zahrnují popis bezpečnostních rad, které by měly všichni zaměstnanci znát, jako je zamykání dveří a skříní, jak lze poznat, že bylo s platebním terminálem manipulováno nebo jak identifikovat oprávněný personál, který přijde terminál servisovat.* | | | | | | | |
| 12.8 | Jsou udržovány a implementovány politiky a postupy pro řízení poskytovatelů služeb, s nimiž jsou data držitelů karet sdílena, nebo kteří by mohli mít vliv na bezpečnost dat držitelů karet, dle následujícího: |  | | | | |
| 12.8.1 | Je udržován seznam poskytovatelů služeb včetně popisu poskytovaných služeb? | * Zkontrolujte politiky a postupy * Sledujte procesy * Zkontrolujte seznam poskytovatelů služeb. |  |  |  |  | |
| 12.8.2 | Je udržována písemná smlouva, která zahrnuje ujednání, že poskytovatelé služeb jsou zodpovědní za bezpečnost dat držitelů karet, kterými poskytovatelé služeb disponují nebo jinak uchovávají, zpracovávají nebo přenášejí jménem zákazníka, nebo v rozsahu, v jakém mohou mít vliv na bezpečnost prostředí dat držitelů karet zákazníka?  ***Poznámka****: Přesné znění ujednání bude záviset na dohodě mezi oběma stranami, s uvedením podrobností o poskytované službě a odpovědnostmi každé strany. Ujednání nemusí obsahovat přesné znění uvedené v tomto požadavku.* | * Sledujte písemné smlouvy * Zkontrolujte politiky a postupy |  |  |  |  | |
| 12.8.3 | Je zajištěno zavedení procesu zapojení poskytovatelů služeb, včetně „due diligence“ před uzavřením závazku? | * Sledujte procesy * Zkontrolujte politiky a postupy a podpůrné dokumentace |  |  |  |  | |
| 12.8.4 | Je udržován program k monitorování stavu shody poskytovatele služeb se standardem PCI DSS nejméně jedenkrát ročně? | * Sledujte procesy * Zkontrolujte politiky a postupy a podpůrné dokumentace |  |  |  |  | |
| 12.8.5 | Jsou udržovány informace o tom, které požadavky PCI DSS jsou spravované každým poskytovatelem služeb, a které jsou řízeny subjektem? | * Sledujte procesy * Zkontrolujte politiky a postupy a podpůrné dokumentace |  |  |  |  | |
| ***Pokyny:*** *Odpovědi „Ano“ na požadavky v 12.8 znamenají, že obchodník má seznam se souhlasy poskytovatelů služeb, se kterými sdílí data držitelů platebních karet. Např. takové souhlasy by byly potřebné v případě, kdy obchodník používá jinou společnost pro uchovávání papírových dokumentů, které obsahují data o účtech zákazníků.* | | | | | | |
| 12.10.1 | (a) Byl vytvořen plán reakce na incident (IRP) tak, aby mohl být implementován v případě události narušení systému? | * Zkontrolujte plán reakce na incident (IRP) * Zkontrolujte postupy plánu reakce na incident (IRP) |  |  |  |  | |
| ***Pokyny:*** *Odpovědi „Ano“ na požadavky v 12.10 znamenají, že obchodník vypracoval plán reakce na incident a jeho eskalaci, používaný v případě nouze, konzistentní s velikostí a komplexností obchodníkových činností. Např. takovýto plán může být jednoduchý backoffice dokument, kde se uvádí komu v jakých situacích zavolat, a který je ročně vyhodnocován tak, aby byl stále přesný, avšak může být rozšířen až na plnohodnotný plán reakce na incident včetně záložních „hotsite“ (plnohodnotná kopie datového centra, která běží zároveň s primárním) zařízení se zevrubnou roční kontrolou. Tento plán by měl být snadno přístupný pro všechen personál v případě nouze.* | | | | | | | |

## Příloha A1: Dodatečné požadavky PCI DSS na poskytovatele sdíleného hostingu

Tato příloha není určena pro obchodníka.

## Příloha A2: Dodatečné požadavky na subjekty používající SSL/dříve TLS pro transakce za fyzické přítomnosti platební karty u POS POI terminálových připojení

Tato příloha není určena pro obchodníka spadajícího do kategorie SAQ A.

Příloha A3: Dodatečné hodnocení pro specifické subjekty DESV (Designated Entities Supplemental Validation)  
  
Tato příloha se týká pouze subjektů určených kartovou společností nebo acquirerem, po kterých je vyžadována další validace stávajících PCI DSS požadavků. Subjekty, od kterých se vyžaduje validace této přílohy, by měly k hlášení využít DESV Supplemental Reporting Template a Supplemental Attestation of Compliance a konzultovat postup jejich podání s příslušnou kartovou společností a/nebo acquirerem.

## 

## Příloha B: Pracovní list náhradního řešení

*Použijte tuto pracovní list k definování náhradních řešení pro každý požadavek, u kterého bylo zaškrtnuto „ANO s CCW“.*

***Poznámka:*** *Pouze společnosti, které podstoupily analýzu rizik a mají legitimní technologické nebo zdokumentované provozní obtíže, mohou při plnění shody uvažovat o náhradních řešeních.*

*Pro více informací o náhradním řešení a pokynech, jak vyplnit tuto pracovní list, se podívejte na přílohy B, C a D standardu PCI DSS.*

**Číslo a definice Požadavku:**

|  |  |  |
| --- | --- | --- |
|  | **Požadovaná informace** | **Vysvětlení** |
| 1. **Omezení** | Seznam omezení znemožňující shodu s původním požadavkem. |  |
| 1. **Cíl** | Definovat cíl původní kontroly, identifikovat cíl splněný kompenzační kontrolou. |  |
| 1. **Identifikované riziko** | Identifikovat jakékoli další riziko způsobené absencí původní kontroly. |  |
| 1. **Definice kompenzační kontroly** | Definovat kompenzační kontroly a vysvětlit, jak jsou řešeny cíle původní kontroly a zvýšená rizika, pokud jsou nějaká. |  |
| 1. **Validace kompenzační kontroly** | Definovat, jak byly kompenzační kontroly ověřeny a testovány. |  |
| 1. **Udržování** | Definovat uplatňované procesy a kontroly k udržování kompenzačních kontrol. |  |

## Příloha C: Vysvětlení pro „Nevztahuje se”(N/A)

*Pokud byl v dotazníku zaškrtnut sloupec “N/A” (Not Applicable), použijte tento pracovní list k vysvětlení, proč související požadavek nelze ve vaší organizaci uplatnit.*

|  |  |
| --- | --- |
| **Požadavek** | **Důvod proč požadavek nelze uplatnit** |
| Příklad: 12.8 | Data držitelů karet nejsou nikdy sdílena s poskytovatelem služeb. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Oddíl 3: Validace a podrobnosti o osvědčení

|  |  |
| --- | --- |
| **Část 3. Ověření podle standardu PCI DSS** | |
| **Toto AOC je založeno na výsledcích uvedených v SAQ P2PE (Část 2), datováno** *(datum vyplnění SAQ),* Na základě výsledků zdokumentovaných v SAQ P2PE poznamenáno výše, podepsané osoby identifikované v části 3b-3d, podle potřeby, potvrzují následující stav shody pro subjekt identifikovaný v části 2 tohoto dokumentu (**zaškrtněte jedno**): | |
|  | **Shoda**: Všechny oddíly dotazníku PCI DSS SAQ jsou vyplněné, na všechny otázky je dána kladná odpověď, takže výsledkem je celkový rating SHODA. Tímto (Název společnosti) prokázal plnou shodu s PCI DSS. |
|  | **Není shoda:** Nejsou vyplněny všechny oddíly dotazníku PCI DSS SAQ nebo na ne všechny otázky je odpověď kladná, takže výsledkem je celkový rating **NENÍ SHODA.** Tímto (Název společnosti)neprokázal plnou shodu s PCI DSS.  **Cílové datum** pro dosažení shody:  Subjekt předkládající tento formulář se statutem „**Není shoda“** může být požádán, aby vyplnil Akční plán v Části 4 tohoto dokumentu. *Před vyplňováním Části 4 postup ověřte u své zpracovatelské banky nebo platební společnosti (platebních společností).* |
|  | **Shoda, ale s právními výjimkami**: U jednoho nebo více požadavků bylo zaškrtnuto „NE“ kvůli právnímu omezení, které znemožňuje splnění konkrétního požadavku. Tato možnost vyžaduje další revizi od zpracovatele (acquirera) nebo platebních asociací.  *Je-li zaškrtnuto, vyplňte následující:*   |  |  | | --- | --- | | **Nesplněný požadavek** | **Detaily, jakým způsobem právní omezení zabraňuje splnění požadavku** | |  |  | |  |  | |

| **Část 3a. Potvrzení stavu** | |
| --- | --- |
| **Podepisující potvrzuje:** *(zaškrtněte vše, co se hodí)* | |
|  | Dotazník pro sebehodnocení P2PE PCI DSS, verze *číslo verze,* byl vyplněn podle pokynů zde uvedených. |
|  | Všechny informace ve výše uvedeném SAQ a v tomto osvědčení věrně zobrazují výsledky mého hodnocení ve všech významných ohledech. |
|  | Přečetl jsem PCI DSS a uznávám, že musím vždy zachovávat udržovat plnou shodu s PCI DSS, příslušnou mému prostředí. |
|  | V případě změny mého prostředí, uznávám, že musím přehodnotit své prostředí a implementovat všechny další potřebné PCI DSS požadavky. |
|  | V ŽÁDNÝCH systémech přezkoumaných během tohoto hodnocení nebyl nalezen žádný důkaz uchovávání dat obsažených na magnetickém proužku (tj. stopě)[[1]](#footnote-1), dat CAV2, CVC2, CID nebo CVV2[[2]](#footnote-2) ani dat PIN[[3]](#footnote-3) po autorizaci transakce |

|  |  |
| --- | --- |
| **Část 3b. Osvědčení obchodníka** | |
|  | |
| *Podpis výkonného ředitele obchodníka* 🡩 | *Datum:* |
| *Jméno výkonného ředitele obchodníka:* | *Funkce:* |

|  |  |  |
| --- | --- | --- |
| **Část 3c. Qualified Security Assessor (QSA) Potvrzení (v případě potřeby)** | | |
| Pokud byl QSA zapojen nebo pomáhal u tohoto hodnocení popište jeho roli: |  | |
|  | | |
| *Podpis řádně pověřeného úředníka QSA společnosti🡩* | | *Datum:* |
| *Jméno řádně pověřeného úředníka:* | | *Společnost QSA:* |
|  | | |
| **Část 3d. Internal Security Assessor (ISA) Potvrzení (v případě potřeby)** | | |
| Pokud byl ISA zapojen nebo pomáhal u tohoto hodnocení, identifikujte ISA osobu a popište jeho roli: |  | |
|  | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Část 4. Akční plán pro požadavky se stavem Není shoda | | | | |
| Vyberte u každého požadavku vhodný „stav shody s požadavky PCI DSS“. Jestliže na kterýkoli z těchto požadavků odpovíte „NE“, může od Vás být požadováno poskytnutí data, kdy Vaše společnost očekává dosažení shody s požadavkem a stručný popis akcí, které se provádějí ke splnění požadavku.  *Před vyplňováním Části 4 postup ověřte u své zpracovatelské banky nebo platební společnosti (platebních společností).* | | | | |
| **Požadavek PCI DSS\*** | **Popis požadavku** | **Statut shody** (vyberte jedno) | | **Datum a akce nápravy** (je-li statut shody  „NENÍ SHODA“) |
| **ANO** | **NE** |
| 3 | Chránit uchovávaná data držitelů karet |  |  |  |
| 9 | Omezit fyzický přístup k datům držitelů karet |  |  |  |
| 12 | Udržovat politiku zaměřenou na informační bezpečnost pro všechen personál |  |  |  |

*\*Zde uvedené PCI DSS požadavky odkazují na otázky v sekci 2 v tomto SAQ.*

**

1. Data zašifrovaná na magnetickém proužku používaná k autorizaci během transakce s přítomností karty. Subjekty si nesmějí ponechat úplná data z magnetického proužku po autorizaci transakce. Jediné prvky dat na stopě, které smějí být zachovány, jsou číslo karty (PAN), datum expirace a jméno držitele karty. [↑](#footnote-ref-1)
2. Trojciferná nebo čtyřciferná hodnota sloužící k ověření transakcí bez přítomnosti karty a vytištěná na podpisovém proužku nebo napravo od něj nebo na lícové straně platební karty. [↑](#footnote-ref-2)
3. Osobní identifikační číslo zadané držitelem karty během transakce s přítomností karty a/nebo zašifrovaný PIN blok uvedený ve zprávě o transakci. [↑](#footnote-ref-3)