

Odvětví platebních karet (PCI)

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

**Obchodníci bez přítomnosti karty, všechny funkce dat držitelů karet zcela outsourcovány**

Pro užití s PCI DSS verze 3.2.1  
  
Revize 1.0.

Červen 2018

# Změny dokumentu

| **Datum** | **Verze** | **Revize SAQ** | **Popis** |
| --- | --- | --- | --- |
| říjen 2008 | 1.2 |  | Sjednocení obsahu dokumentu s novým Standardem bezpečnosti dat odvětví platebních karet v. 1.2 a implementování menší změny zaznamenané od vydání původní verze v. 1.1. |
| říjen 2010 | 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). |
| červenec 2015 | 3.1 | 1.1 | Aktualizace číslování verze za účelem sjednocení s ostatními SAQ dotazníky. |
| 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). Přidány požadavky z PCI DSS v3.2, požadavky 1,5,6,7,8,10,11 a příloha A2. |
| leden 2017 | 3.2 | 1.1 | Aktualizace změn dokumentu, aby odrážel požadavky přidané v aktualizaci duben 2016  Přidána poznámka k sekci „Než začnete“ k vysvětlení záměrů zahrnutí požadavků PCI DSS č. 2 a 8. |
| 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).  Přidán požadavek 6.2 z PCI DSS v3.2.1. |

# Obsah

[Změny dokumentu 1](#_Toc13755031)

[Obsah 2](#_Toc13755032)

[Než začnete 3](#_Toc13755033)

[PCI DSS – Postup vyplnění sebehodnotícího dotazníku 4](#_Toc13755034)

[Jak porozumět sebehodnotícímu dotazníku 4](#_Toc13755035)

[Očekávané Testování 4](#_Toc13755036)

[Vyplnění sebehodnotícího dotazníku 5](#_Toc13755037)

[Postup v případech, kdy nelze aplikovat určité specifické požadavky 5](#_Toc13755038)

[Výjimky ze zákona 5](#_Toc13755039)

[Oddíl 1: Informace o hodnocení 6](#_Toc13755040)

[Oddíl 2: Dotazník pro sebehodnocení A 9](#_Toc13755041)

[Požadavek 2: Nepoužívat výchozí nastavení od dodavatele pro systémová hesla a jiné bezpečnostní parametry 9](#_Toc13755042)

[Požadavek 6: Vyvíjet a udržovat bezpečné systémy a aplikace 10](#_Toc13755043)

[Požadavek 8: Identifikovat a autentizovat přístup k systémovým komponentám 11](#_Toc13755044)

[Požadavek 9: Omezit fyzický přístup k datům držitelů karet 12](#_Toc13755045)

[Udržování politiky bezpečnosti informací 13](#_Toc13755046)

[Požadavek 12: Udržovat politiku zaměřenou na informační bezpečnost pro všechen personál 13](#_Toc13755047)

[Příloha A1: Dodatečné požadavky PCI DSS na poskytovatele sdíleného hostingu 14](#_Toc13755048)

[Příloha A2: Dodatečné požadavky na subjekty používající SSL/dříve TLS pro transakce za fyzické přítomnosti platební karty u POS POI terminálových připojení 14](#_Toc13755049)

[Příloha A3: Dodatečné hodnocení pro specifické subjekty DESV (Designated Entities Supplemental Validation) 14](#_Toc13755050)

[Příloha B: Pracovní list náhradního řešení 15](#_Toc13755051)

[Příloha C: Návod pro „Nevztahuje se”(N/A) 16](#_Toc13755052)

[Oddíl 3: Validace a podrobnosti o osvědčení 17](#_Toc13755053)

# 

# Než začnete

SAQ A byl vypracován tak, aby zohlednil požadavky vztahující se na obchodníky, kteří mají veškeré funkce týkající se dat držitelů karet dodány od ověřeného dodavatele služeb (třetí stranou, kde obchodník drží pouze papírové záznamy a účtenky s daty držitelů karet.

SAQ A obchodníci mohou být buď e-commerce nebo MO/TO obchodníci (karta nepřítomna), kteří neuchovávají, nezpracovávají, nebo nepřenášejí žádná data držitelů karet v elektronické podobě ve svých systémech, úložištích nebo prostorách.

SAQ A obchodníci potvrzují, že pro tento platební kanál:

* Vaše společnost zpracovává pouze transakce bez přítomnosti karty (card-not-present), tj. e-commerce nebo písemné/telefonní objednávky;
* veškeré přijímání a zpracování dat držitelů karet je zcela zabezpečeno třetí stranou – poskytovatelem služeb prověřeným z hlediska PCI DSS;
* Vaše společnost elektronicky neuchovává, nezpracovává nebo nepřenáší žádná data držitelů karet ve svých systémech, úložištích nebo prostorách, ale bezvýhradně spoléhá na zajištění těchto funkcí třetí stranou;
* Vaše společnost má potvrzeno, že všechny třetí strany zajišťující ukládání, zpracování a/nebo přenos dat držitelů karet, jsou v souladu s PCI DSS;
* jakákoliv data držitelů karet, která Vaše společnost uchovává jsou v papírové podobě (např. papírové záznamy nebo papírové kopie účtenek) a tyto dokumenty nejsou přijímány elektronicky.

*Navíc pro e-commerce kanály:*

* Všechny části stránek s platebními údaji, které zákazníci vidí na svých prohlížečích, pocházejí pouze přímo od PCI DSS prověřeného poskytovatele služeb – třetí strany.

***Tento SAQ se nevztahuje na face-to-face 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.

***Poznámka:*** *Požadavky PCI DSS v tomto SAQ, které se zabývají ochranou počítačových systémů (například požadavky č. 2,6,8) platí pro e-commerce obchodníky, kteří přesměrovávají zákazníky ze své webové stránky na stránky třetích stran kvůli zpracování platby a zejména na server obchodníka, na kterém je lokalizován systém přesměrování. Na obchodníky uzavírající objednávky poštou či telefonem nebo e-commerce obchodníky, kteří všechny úkony outsourcují (a není zde žádní mechanismus přesměrování od obchodníka k třetím stranám), tudíž nemají žádné systémy v spadající do rozsahu tohoto SAQ, se tyto požadavky nemusí vztahovat.” Viz. Návod jak uvést požadavky, které se na Vás nevztahují, na následujících stránkách.*

## PCI DSS – Postup vyplnění sebehodnotícího dotazníku

1. Nalezněte příslušný SAQ pro vaše prostředí – více naleznete v dokumentu Návody a pokyny k dotazníku pro sebehodnocení (*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 - AOC).
3. Posuďte, zda je vaše prostředí v souladu s příslušnými požadavky PCI DSS.
4. Vyplňte všechny části tohoto dokumentu:

* Oddíl 1 (Část 1 & 2 AOC) – Informace o hodnocení a Shrnutí
* Oddíl 2 – PCI DSS sebehodnotící dotazník (SAQ A)
* 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 (AOC - Attestation of Compliance) spolu s další požadovanou dokumentací – jako je například „ASV scan report“ – vaší zpracovatelské 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 ohodnocení.

### 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. ***Pouze jedna odpověď by měla být vybrána 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 určité specifické požadavky

V případě, že některý z požadavků nelze aplikovat na vaše prostředí, vyberte u daného požadavku možnost „N/A“ a vyplňte „Explanation of Non-Applicability“ (Návod 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: Obchodník je zodpovědný za to, aby každá část byla vyplněna relevantními stranami. Kontaktujte acquirera (zpracovatelskou banku obchodníka) nebo kartové společnosti aby stanovily reporting a způsob předložení.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Část 1. Informace o obchodníkovi a společnosti kvalifikovaných hodnotitelů bezpečnosti** | | | | | | | |
| **Část 1a. Informace o společnosti obchodníka** | | | | | | | |
| 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** | | | | |
| Používá společnost jednu nebo více platebních aplikací?  Ano  Ne | | | | |
| Poskytněte následující informace týkající se platebních aplikací, které vaše společnost používá: | | | | |
| **Název platební aplikace** | **Číslo verze** | **Dodavatel aplikace** | **Je aplikace na seznamu PA-DSS?** | **Expirace PA-DSS (je-li to relevantní)** |
|  |  |  | Ano  Ne |  |
|  |  |  | Ano  Ne |  |
|  |  |  | Ano  Ne |  |
|  |  |  | Ano  Ne |  |
|  |  |  | Ano  Ne |  |

|  |  |  |
| --- | --- | --- |
| **Část 2e. Popis prostředí** | | |
| Poskytněte „**high-level**“ popis vašeho prostředí, na které se vztahuje toto hodnocení.  *Například:*   * *Spojení dovnitř a ven 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** | | |
| Využívá 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 A** | |
| Obchodník potvrzuje, že je způsobilý k vyplnění této zkrácené verze Dotazníku pro sebehodnocení, protože pro tento platební kanál: | |
|  | Obchodník přijímá pouze card-not-present (e-commerce nebo MO/TO) transakce. |
|  | Veškeré zpracování dat držitelů karet je zcela zabezpečeno poskytovatelem služeb – třetí stranou prověřenou z hlediska PCI DSS. |
|  | Obchodník elektronicky neuchovává, nezpracovává ani nepřenáší jakákoli data držitelů karet na svých systémech nebo prostorách, ale při provádění těchto funkcí se plně opírá o poskytovatele služeb – třetí stranu. |
|  | Obchodník má potvrzeno, že všechny třetí strany zajišťující uchovávání, zpracování a/nebo přenos dat držitelů karet, jsou v souladu s PCI DSS; |
|  | Obchodník uchovává pouze papírové záznamy nebo účtenky s jakýmikoliv daty držitelů karet a tyto dokumenty nejsou přijímány elektronicky. |
|  | *Dodatečně, pro e-commerce kanály:*  Všechny prvky stránek s platebními údaji, které zákazníci vidí na svých prohlížečích, pocházejí pouze přímo od poskytovatele služeb – třetí strany prověřené z hlediska PCI DSS. |

# Oddíl 2: Dotazník pro sebehodnocení A

|  |
| --- |
| ***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:**

### Požadavek 2: Nepoužívat výchozí nastavení od dodavatele pro systémová hesla a jiné bezpečnostní parametry

| **PCI DSS Otázka** | | **Očekávané Testování** | **Odpověď**  **(zaškrtněte jednu odpověď pro každou otázku)** | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **ANO** | **ANO s „CCW“** | **NE** | **N/A** |
| 2.1 | (a) Jsou vždy změněna výchozí (defaultní) nastavení od dodavatelů před instalací systémů do sítě?  *To se vztahuje na VŠECHNA výchozí (defaultní) hesla, kromě jiných i na ta, používaná pro operační systémy, software poskytující bezpečnostní služby, aplikační a systémové účty, point-of-sale (POS) terminály, platební aplikace, Simple Network Management Protocol (CNMP) Community strings (Pozn. překl.: Obdoba hesel pro přístup do statistik routeru.) apod.* | * Zkontrolujte politiky a postupy * Přezkoumejte dokumentace dodavatelů * Sledujte systémové konfigurace a nastavení účtů * Rozhovor s personálem |  |  |  |  |
| (b) Jsou všechny zbytečné výchozí (defaultní) účty odstraněny nebo deaktivovány před instalací systémů do sítě? | * Zkontrolujte politiky a postupy * Přezkoumejte dokumentace dodavatelů * Přezkoumejte konfigurace systému a nastavení účtů * Rozhovor s personálem |  |  |  |  |

### Požadavek 6: Vyvíjet a udržovat bezpečné systémy a aplikace

| **PCI DSS Otázka** | | **Očekávané Testování** | **Odpověď**  **(zaškrtněte jednu odpověď pro každou otázku)** | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **ANO** | **ANO s „CCW“** | **NE** | **N/A** |
| 6.2 | (a) Jsou všechny komponenty systémů a softwaru chráněny proti známým zranitelnostem instalováním vhodných bezpečnostních záplat dodaných dodavatelem? | * Zkontrolujte politiky a postupy |  |  |  |  |
|  | (b) Jsou kritické bezpečnostní záplaty instalovány v průběhu jednoho měsíce od zpřístupnění?  ***Poznámka****: Kritické bezpečnostní záplaty by měly být identifikovány podle procesu klasifikace rizik definovaného v Požadavku 6.1.* | * Zkontrolujte politiky a postupy * Přezkoumejte komponenty systémů * Porovnejte seznam instalovaných bezpečnostních záplat se seznamem záplat aktuálně vydaných dodavatelem |  |  |  |  |

### Požadavek 8: Identifikovat a autentizovat přístup k systémovým komponentám

| **PCI DSS Otázka** | | **Očekávané Testování** | **Odpověď**  **(zaškrtněte jednu odpověď pro každou otázku)** | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **ANO** | **ANO s „CCW“** | **NE** | **N/A** |
| 8.1.1 | Jsou přiděleny všem uživatelům jedinečné uživatelské ID před umožněním jejich přístupu k systémovým komponentám nebo datům držitelů karet? | * Zkontrolujte postupy pro hesla * Rozhovor s personálem |  |  |  |  |
| 8.1.3 | Jsou ihned rušeny nebo deaktivovány přístupy každému uživateli, jehož přístupové oprávnění bylo ukončeno? | * Zkontrolujte postupy pro hesla * Přezkoumejte účty zrušených uživatelů * Zkontrolujte aktuální seznamy přístupů * Sledujte navrácená fyzická autentizační zařízení |  |  |  |  |
| 8.2 | Je kromě přidělení jedinečného uživatelského ID využívána jedna nebo více z následujících metod k ověření všech uživatelů?   * Něco, co znáte – jako je heslo nebo heslová fráze * Něco, co máte – jako je token nebo čipová karta * Něco, kým jste – například biometrika. | * Zkontrolujte postupy pro hesla * Sledujte autentizační procesy |  |  |  |  |
| 8.2.3 | (a) Jsou parametry hesla / heslové fráze nastaveny tak, aby vyhovovaly následujícímu?   * minimální délka hesla je nejméně sedm znaků * obsahuje jak numerické, tak abecední znaky.   Alternativně musí mít hesla / heslové fráze složitost a sílu, která je alespoň rovnocenná parametrům uvedených výše. | * Přezkoumejte nastavení konfigurace systémů pro ověření parametrů hesel |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 8.5 | Jsou zakázány skupinové, sdílené či generické účty, hesla nebo jiné autentizační metody dle následujícího:   * Generická ID uživatele a účty jsou zakázány nebo odstraněny. * Neexistují sdílená ID uživatele pro činnosti zprávy systému a dalších kritických funkcí. * Sdílená a generická ID uživatele nejsou používána k správě jakýchkoli systémových komponent? | * Zkontrolujte politiky a postupy * Přezkoumejte seznamy ID uživatelů * Rozhovor s personálem |  |  |  |  |

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

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **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 |  |  |  |  |
| 9.6 | | (a) Je zavedena a udržována pro jakékoli druhy médií přísná vnitřní i vnější kontrola distribuce? | * Zkontrolujte politiky a postupy pro distribuci médií |  |  |  |  |
|  | | (b) Zahrnují kontroly následující: |  | | | | |
| 9.6.1 | | Jsou média klasifikována tak, aby mohla být identifikována citlivost dat? | * Zkontrolujte politiky a postupy pro klasifikaci médií * Rozhovor s bezpečnostním personálem |  |  |  |  |
| 9.6.2 | | Jsou média zasílána bezpečným kurýrem nebo jinou zasílací metodou, která může být přesně sledována? | * Rozhovor s personálem * Přezkoumejte dokumentaci a záznamy sledování distribuce médií |  |  |  |  |
| 9.6.3 | | Schválil management všechna média, která jsou přesouvána mimo bezpečnou oblast (včetně médií distribuovaných jednotlivcům)? | * Rozhovor s personálem * Přezkoumejte dokumentaci a záznamy sledování distribuce médií |  |  |  |  |
| 9.7 | | Je udržována přísná kontrola nad ukládáním a dostupností médií? | * Zkontrolujte politiky a postupy |  |  |  |  |
| 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 |  |  |  |  |

## Udržování politiky bezpečnosti informací

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

***Poznámka:*** *Pro účely požadavku 12 se „personálem“ rozumí zaměstnanci pracující na plný i zkrácený úvazek, na dobu určitou, i kontraktoři a konzultanti, kteří mají přístup do systémů a prostředí obsahujících data držitelů karet (CDE).*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **PCI DSS Otázka** | | **Očekávané Testování** | **Odpověď**  **(zaškrtněte jednu odpověď pro každou otázku)** | | | |
| **ANO** | **ANO s „CCW“** | **NE** | **N/A** |
| 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 |  |  |  |  |
| 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) |  |  |  |  |

## 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: Návod 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:3.4 | Data držitelů karet nejsou nikdy ukládána elektronicky |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Oddíl 3: Validace a podrobnosti o osvědčení

|  |  |  |
| --- | --- | --- |
| **Část 3. Ověření podle standardu PCI DSS** | | |
| **Toto AOC je založeno na výsledcích uvedených v SAQ A (Část 2), datováno** *( datum dokončení SAQ),* Na základě výsledků zdokumentovaných v SAQ A 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 A PCI DSS, verze *číslo verze dotazníku,* 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. | |
|  | | | Potvrdil jsem společně se svým dodavatelem platební aplikace, že platební systém neuchovává citlivá autentizační data po autorizaci | |
|  | | | 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 | |
|  | | | ASV skeny jsou vyhotoveny PCI SSC schváleným dodavatelem skenováníASV(PCI SSC Approved Scanning Vendor) (ASV název) | |

|  |  |
| --- | --- |
| **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** | **Stav shody s PCI DSS  (vyberte jedno)** | | **Datum a akce nápravy (je-li stav shody pro nějaký požadavek „NE“)** |
| **ANO** | **NE** |
| 2 | Nepoužívat výchozí nastavení od dodavatele pro systémová hesla a jiné bezpečnostní parametry |  |  |  |
| 6 | Vyvíjet a udržovat bezpečné systémy a aplikace |  |  |  |
| 8 | Identifikovat a autentizovat přístup k systémovým komponentám |  |  |  |
| 9 | Omezit fyzický přístup k datům držitelů karet |  |  |  |
| 12 | Udržovat politiku zaměřenou na informační bezpečnost pro všechen personál |  |  |  |

\* Zde uvedené požadavky PCI DSS se vztahují k otázkám v Oddílu 2 dotazníku 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)