

Obowiązek zgodności ze standardem bezpieczeństwa PCI DSS

Od 1 kwietnia 2024 roku wszyscy Akceptanci powinni być w pełni zgodni z wymogami standardu PCI DSS (obecnie wersja 4.0).

1. Kryteria określenia sposobów kontroli zgodności z PCI DSS

Grupa 1	Metody weryfikacji zgodności z PCI DSS
> roczna liczba transakcji powyżej 6 mln w systemie Visa lub Mastercard > inni Akceptanci o podwyższonym ryzyku wyznaczeni decyzją systemów płatniczych	> coroczny Audyt PCI > kwartalny Zewnętrzny Skan Sieci ASV
Grupa 2	
> roczna liczba transakcji od 1 mln do 6 mln w systemie Visa lub Mastercard	> coroczna Samoocena Zgodności PCI* > kwartalny Zewnętrzny Skan Sieci ASV
Grupa 3	
> roczna liczba transakcji eCommerce (handel elektroniczny) od 20 tys. do 1 mln w systemie Visa lub Mastercard	> coroczna Samoocena Zgodności PCI > kwartalny Zewnętrzny Skan Sieci ASV (jeżeli dotyczy)
Grupa 4	
> pozostali Akceptanci	> coroczna Samoocena Zgodności PCI (tylko na prośbę agenta rozliczeniowego) > kwartalny Zewnętrzny Skan Sieci ASV (jeżeli dotyczy i tylko na prośbę agenta rozliczeniowego)

* Akceptanci, którzy spełniają kryteria SAQ A, A-EP i/lub D (patrz pkt 4 poniżej), muszą skorzystać z usług QSA (Qualified Security Assessor) / ISA (Internal Security Assessor) w ramach Samooceny Zgodności PCI i/lub Audytu PCI. Akceptanci, którzy spełniają kryteria SAQ B, B-IP, C, C-VT i/lub P2PE mogą opcjonalnie skorzystać z usług QSA / ISA w ramach Samooceny Zgodności PCI, czyli uzupełnienia kwestionariusza samooceny typu SAQ.

2. Metody weryfikacji zgodności z PCI DSS, o których mowa powyżej:

- > Audyt PCI – Audyt zgodności z PCI przeprowadzony przez zewnętrznego Certyfikowanego Audytora Bezpieczeństwa (ang. QSA – Qualified Security Assessor).
- > Lista firm oferujących usługi QSA w Polsce dostępna jest na stronie PCI DSS: https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors.

- > Samoocena Zgodności PCI (szczegóły pkt 4).
- > Kwartałny Zewnętrzny Skan Sieci ASV (szczegóły pkt 3).

3. Zewnętrzny Skan Sieci

- > Zewnętrzny Skan Sieci wykonywany jest przez firmy wyznaczone przez PCI DSS. Lista takich firm (ang. ASV – Approved Scanning Vendor) dostępna jest na stronie PCI DSS:

https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors

4. Samoocena Zgodności PCI

Samoocena Zgodności PCI (ang. SAQ – Self-Assessment Questionnaire) jest dokumentowana w kwestionariuszu samooceny SAQ.

Rodzaj wypełnianego kwestionariusza SAQ zależy do rozwiązań technologicznych stosowanych przez Akceptanta:

Opis rozwiązań technologicznych stosowanych przez Akceptanta	Typ kwestionariusza samooceny SAQ
Akceptant, który przeprowadza transakcje bez fizycznej obecności karty płatniczej (eCommerce lub MO/TO) i który w całości przetwarzanie danych kart płatniczych powierza zewnętrznemu dostawcy usług posiadającemu certyfikat PCI DSS, przy czym Akceptant nie przechowuje danych kart płatniczych w formie elektronicznej, nie przesyła ani nie przetwarza ich w zakresie swoich systemów informatycznych. (Stosuje się wyłącznie do przypadków, gdy Akceptant przyjmuje płatności internetowe).	A
Akceptant przyjmujący transakcje za pośrednictwem Internetu (eCommerce), który w całości przetwarzanie danych kart płatniczych powierza zewnętrznemu dostawcy usług posiadającemu certyfikat PCI DSS, przy czym Akceptant nie przechowuje danych kart płatniczych w formie elektronicznej, nie przesyła ani nie przetwarza ich w swoich systemach informatycznych lub na swoim terenie oraz nie pobiera danych kart płatniczych za pośrednictwem swojej strony internetowej, jednak stopień zabezpieczenia tej strony może mieć wpływ na bezpieczeństwo transakcji dokonywanych kartą płatniczą. (Stosuje się wyłącznie do przypadków, gdy Akceptant przyjmuje płatności internetowe).	A-EP
Akceptant korzystający wyłącznie z: • z urządzeń typu Imprinter i/lub • z wolnostojących terminali łączących się za pośrednictwem telefonii stacjonarnej, przy czym Akceptant nie przechowuje danych kart płatniczych w formie elektronicznej. (Nie stosuje się do przypadków, gdy Akceptant przyjmuje płatności internetowe).	B

Akceptant korzystający wyłącznie z wolnostojących terminali posiadających certyfikat PCI-PTS łączących się z użyciem protokołu IP, bez przechowywania danych kart płatniczych w formie elektronicznej.

(Nie stosuje się do przypadków, gdy Akceptant przyjmuje płatności internetowe).

B-IP

Akceptant, który wykorzystuje aplikację płatniczą opartą na systemie informatycznym podłączonym do Internetu. Akceptant nie przechowuje danych kart płatniczych w formie elektronicznej.

(Nie stosuje się do przypadków, gdy Akceptant przyjmuje płatności internetowe).

C

Akceptant, który wprowadza transakcje ręcznie do wirtualnego terminala udostępnianego przez Internet i zarządzanego przez zewnętrznego dostawcę usług, posiadającego certyfikat PCI DSS. Akceptant nie przechowuje danych kart płatniczych w formie elektronicznej.

(Nie stosuje się do przypadków, gdy Akceptant przyjmuje płatności internetowe).

C-VT

Akceptant korzystający wyłącznie z wolnostojących terminali wykorzystujących i zarządzanych przez zaakceptowane przez PCI SSC rozwiązanie P2PE. Akceptant nie przechowuje danych kart płatniczych w formie elektronicznej.

(Nie stosuje się do przypadków, gdy Akceptant przyjmuje płatności internetowe).

P2PE

Sprzedawcy korzystający z komercyjnego, gotowego urządzenia mobilnego (na przykład telefonu lub tabletu) z bezpiecznym czytnikiem kart znajdującym się na liście zatwierdzonych rozwiązań SPoC PCI SSC. Akceptant nie ma dostępu do danych kart płatniczych w formie jawnej i nie przechowuje danych kart płatniczych w formie elektronicznej.

(Nie stosuje się do przypadków, gdy Akceptant przyjmuje płatności internetowe i/lub MO/TO).

SPoC

Wszyscy pozostali Akceptanci z dostępem do danych kartowych i/lub nie zakwalifikowani do kategorii wymienionej powyżej.

D

> Kwestionariusze SAQ dostępne są na stronie:

https://www.pcisecuritystandards.org/document_library?category=sags#results

> Akceptanci z Grupy 2, Grupy 3 i Grupy 4 mogą wypełnić formularz SAQ samodzielnie. Akceptanci z Grupy 2 muszą wypełnić formularz SAQ (i/lub mogą przeprowadzić Audyt PCI) przy pomocy QSA lub swojego pracownika, który uzyskał tytuł ISA (Internal Security Assessor) tylko i wyłącznie w przypadku SAQ A, A-EP i D. Sposób uzyskania kwalifikacji ISA jest opisany na stronie PCI DSS:

https://www.pcisecuritystandards.org/program_training_and_qualification/internal_security_assessor_certification.

5. Niezbędne informacje dotyczące PCI DSS

- > PCI DSS – Wymagania – Dokument do pobrania w aktualnej wersji standardu:
https://www.pcisecuritystandards.org/document_library
- > PCI DSS – materiały edukacyjne dla Akceptantów i Service Providerów:
https://www.pcisecuritystandards.org/pci_security/educational_resources
- > PCI DSS – formularze SAQ oraz Przewodnik do ich wypełnienia:
https://www.pcisecuritystandards.org/document_library?category=sags#results
- > PCI DSS – lista kwalifikowanych audytorów:
https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors
- > PCI DSS – lista kwalifikowanych firm prowadzących skanowanie sieci:
https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors
- > Stron główna PCI Council (PCI SSC):
<https://www.pcisecuritystandards.org/index.php>
- > Informacje źródłowe z Mastercard:
<https://www.mastercard.us/en-us/business/overview/safety-and-security/security-recommendations/site-data-protection-PCI/merchants-need-to-know.html>
- > Informacje źródłowe z VISA:
<https://usa.visa.com/support/small-business/security-compliance.html>