Сертификация облачного сервиса как элемента платежной инфраструктуры в соответствии с требованиями PCI DSS

Содержание

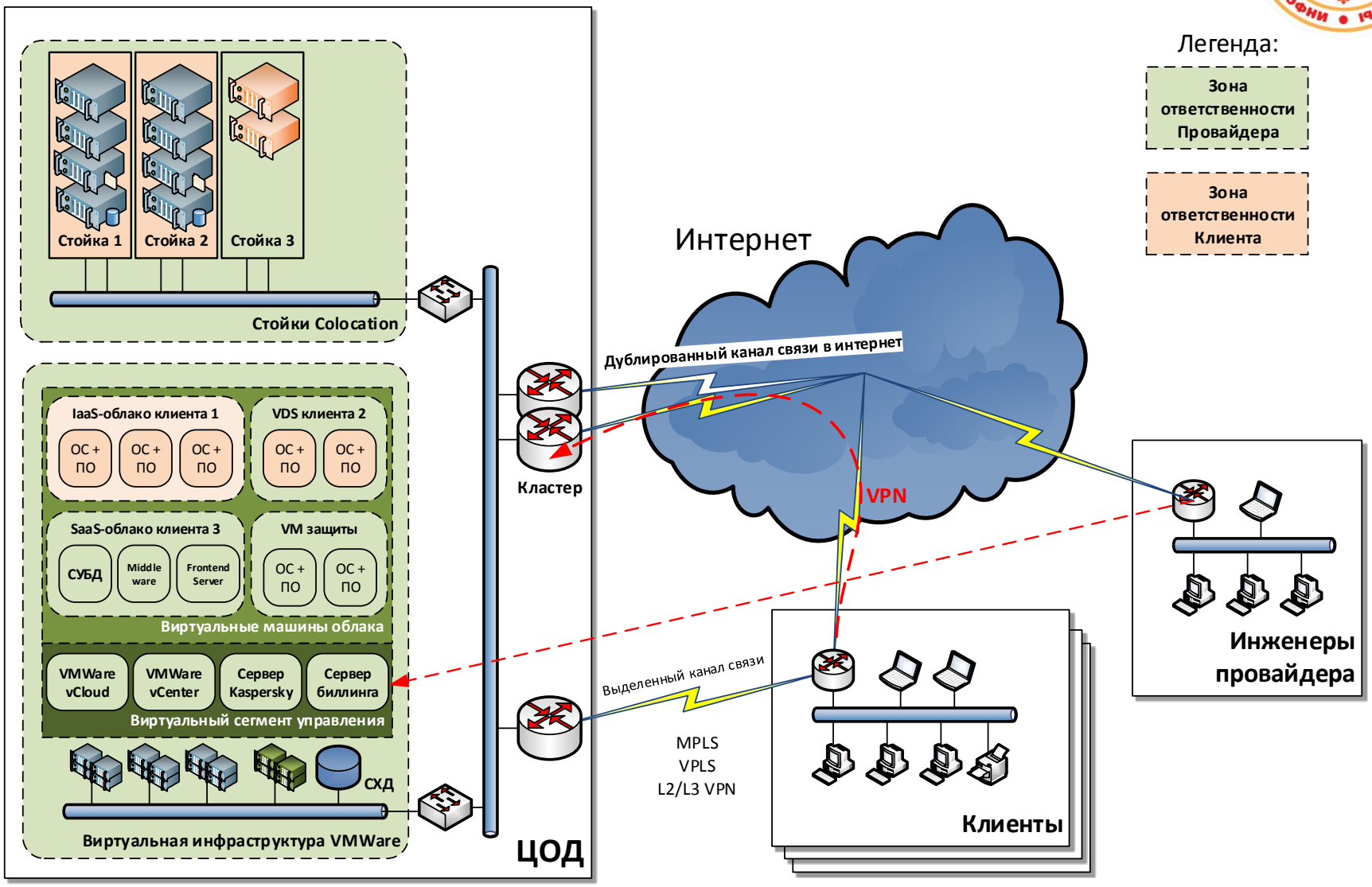
- Почему облачный сервис должен проходить сертификацию
- Сервисы, входящие в область сертификации PCI DSS 3.0 и группы требований
- Этапность выполнения работ по сертификации облачного сервиса
- Обеспечение соответствия и планы развития сертифицированного облачного сервиса

Почему облачный сервис должен проходить сертификацию

- Классификация МПС определяет два типа организаций:
  - Торгово-сервисные предприятия;
  - Поставщики услуг.
- Классификация МПС для поставщиков услуг:

Уровень	Критерии
1	• Обработка более 300 тыс. транзакций в год, или • Процессинг, подключенный напрямую к VISANet, независимо от количества транзакций (VISA) • Внешний процессинг, независимо от количества транзакций
2	• Обработка менее 300 тыс. транзакций в год

Инфраструктура облачного сервиса



Преимущества использования сертифицированного облачного сервиса

- Снижение CAPEX на создание своего ЦОД
- Снижение затрат на обслуживание инфраструктуры в рамках SLA
- Исключение из области сертификации заказчика элементов инфраструктуры, размещенных в облачном сервисе
- Перенос рисков в случае инцидентов с проведением платежей

Формат соответствия

Уровень	Подтверждение соответствия
1	• QSA ежегодно • ASV ежеквартально
2	• SAQ ежегодно • ASV ежеквартально

- QSA – внешний аудит, выполняется внешней аудиторской организацией (Qualified Security Assesor, QSA), сертифицированной Советом PCI SSC.
- SAQ – самооценка, выполняется самостоятельно путем заполнения листа самооценки (Self-Assessment Questionnaire, SAQ).
- ASV – тестирование безопасности информационных систем, входящих в область требований PCI DSS и имеющих выход в Интернет (межсетевые экраны, почтовые серверы, web-приложения, DNS-серверы и т.д. специализированным сканером (Approved Scanning Vendor, ASV)

Разновидности самооценки и количество требований PCI DSS 3.0

Вариант	Применимость	Количество требований
SAQ A	Мерченты, выполняющие card-not-present транзакции, отдавшие все функции по вводу и обработке данных платежных карт на аутсорсинг поставщику услуг, подтвердившему соответствие PCI DSS, и не имеющие возможность повлиять на безопасность платежных транзакций.	14
SAQ A-EP	Мерченты, выполняющие card-not-present транзакции, отдавшие все функции по передаче, обработке и хранению данных платежных карт на аутсорсинг поставщику услуг, подтвердившему соответствие PCI DSS, и при этом способные повлиять на безопасность платежных транзакций.	139
SAQ D	Все мерчанты и поставщики услуг, кроме тех, кому согласно требования МПС или эквайера необходим ISA- или QSA-аудит.	329

Сервисы, входящие в область сертификации PCI DSS 3.0

Name of service(s) assessed:	Virtual hosting	
Type of service(s) assessed:		
Hosting Provider: ☐ Applications / software ☒ Hardware ☒ Infrastructure / Network ☒ Physical space (co-location) ☐ Storage ☐ Web ☐ Security services ☐ 3-D Secure Hosting Provider ☒ Shared Hosting Provider ☒ Other Hosting (specify): Virtual (VMware) infrastructure	**Managed Services (specify):** ☐ Systems security services ☐ IT support ☒ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☐ POS / card present ☐ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☐ Other processing (specify):
☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☐ Others (specify):		

Группы требований

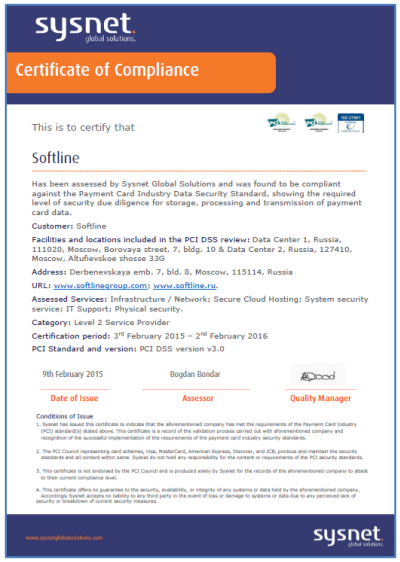
№	Требования PCI DSS	Детали оценки			
		Полностью	Частично	Неприменимо	Комментарий
1	Защита вычислительной сети		✓		1.2.3 Неприменимо, так как беспроводные сети не используются 1.4 Неприменимо, так как использование персональных устройств не входит в область проверки
2	Конфигурация компонентов		✓		2.1.1 Неприменимо, так как беспроводные сети не используются 2.3.e Неприменимо, так как POS-терминалы не используются
3	Защита хранимых данных			✓	Данные о держателях карт не хранятся
4	Защита передаваемых данных			✓	Данные о держателях карт не передаются
5	Антивирусная защита	✓			
6	Разработка и поддержка ИС		✓		6.3-6.3.2, 6.5.5.3.b, 6.5-6.6 Неприменимо, так как нет средств разработки ПО
7	Управление доступом к данным	✓			
8	Механизмы аутенитификации		✓		8.1.5a-8.1.5.b Неприменимо, так как нет удаленного доступа у разработчиков ПО (вендоров)

Группы требований. Окончание

№	Требования PCI DSS	Детали оценки			
		Полностью	Частично	Неприменимо	Комментарий
9	Физическая защита			✓	Датацентр обеспечивает все применяемые подтребования из группы согласно Матрицы ответственности между Датацентром и облачным провайдером 9.9-9.9.3 Неприменимо, так как отсутствуют POS-терминалы
10	Протоколирование событий		✓		10.2.1 Неприменимо, так как данные о держателях карт не сохраняются
11	Контроль защищенности			✓	Датацентр обеспечивает все применяемые подтребования 11.1-11.1.2 из группы согласно Матрицы ответственности между Датацентром и облачным провайдером
12	Управление ИБ		✓		12.3.1-12.3.10.b Неприменимо, так как критичные технологии не применяются
	Приложение А	✓			

Динамика оценки соответствия облачного сервиса требованиям PCI DSS

Год	Уровень	Способ оценки	Пройденные процедуры	Документы соответствия
2015	2	SAQ	• Заполнение листа самооценки • ASV-сканирование	• SAQ • AOC • Certificate
2016	1	QSA-аудит	• Предварительный аудит • ASV-сканирование • Тест на проникновение	• ROC • AOC • Certificate


sysnet global solutions

Certificate of Compliance

This is to certify that

Softline

Has been assessed by Sysnet Global Solutions and was found to be compliant against the Payment Card Industry Data Security Standard, showing the required level of security due diligence for storage, processing and transmission of payment card data.

Customer: Softline

Facilities and locations included in the PCI DSS review: Data Center 1, Russia, 111020, Moscow, Borovaya street, 7, bldg. 10 & Data Center 2, Russia, 127410, Moscow, Altufievskoe shosse 33G

Address: Derbenevskaya emb. 7, bld. 8, Moscow, 115114, Russia

URL: www.softlinegroup.com; www.softline.ru

Assessed Services: Infrastructure / Network; Secure Cloud Hosting; System security service; IT Support; Physical security.

Category: Level 2 Service Provider

Certification period: 3rd February 2015 – 2nd February 2016

PCI Standard and version: PCI DSS version v3.0

9th February 2015	Bogdan Bondar	
Date of Issue	Assessor	Quality Manager

Conditions of Issue

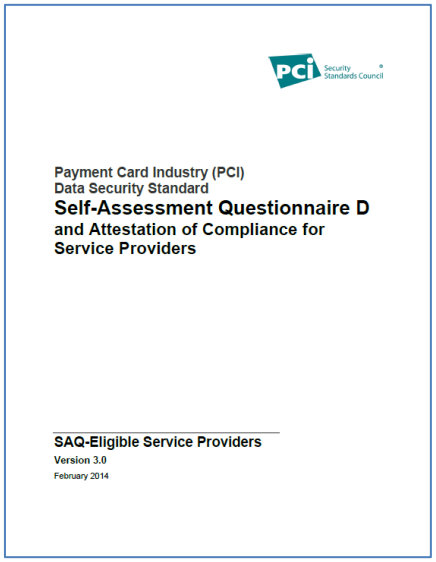
1. Sysnet has issued this certificate to indicate that the aforementioned company has met the requirements of the Payment Card Industry (PCI) standard(s) stated above. This certificate is a record of the validation process carried out with aforementioned company and recognition of the successful implementation of the requirements of the payment card industry security standards.

2. The PCI Council representing card schemes, Visa, MasterCard, American Express, Discover, and JCB, produce and maintain the security standards and all content within same. Sysnet do not hold any responsibility for the content or requirements of the PCI security standards.

3. This certificate is not endorsed by the PCI Council and is produced solely by Sysnet for the records of the aforementioned company to attest to their current compliance level.

4. This certificate offers no guarantee to the security, availability, or integrity of any systems or data held by the aforementioned company. Accordingly Sysnet accepts no liability to any third party in the event of loss or damage to systems or data due to any perceived lack of security or breakdown of current security measures.

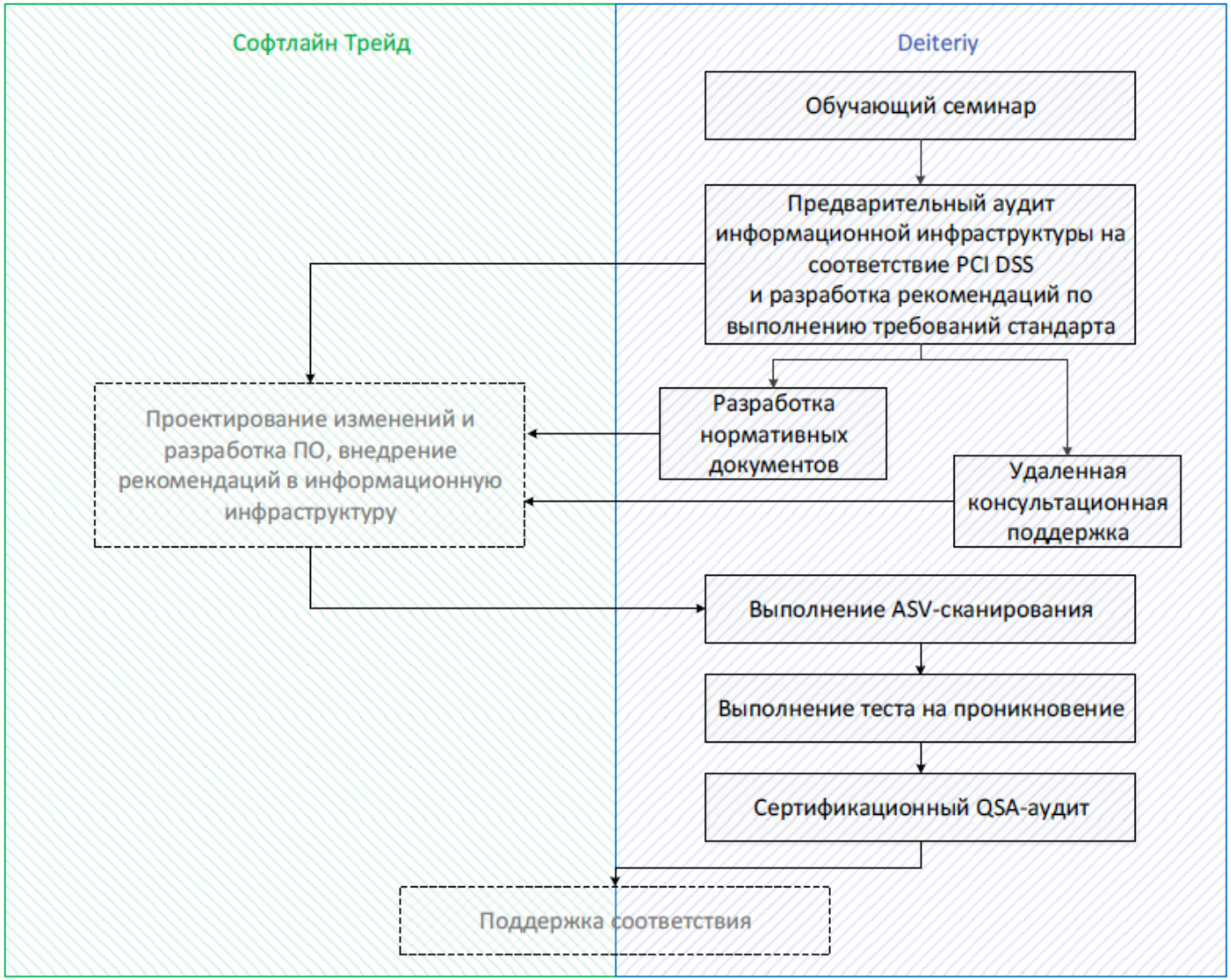
sysnet global solutions


PCI Security Standards Council

Payment Card Industry (PCI)
Data Security Standard
Self-Assessment Questionnaire D
and Attestation of Compliance for Service Providers

SAQ-Eligible Service Providers
Version 3.0
February 2014

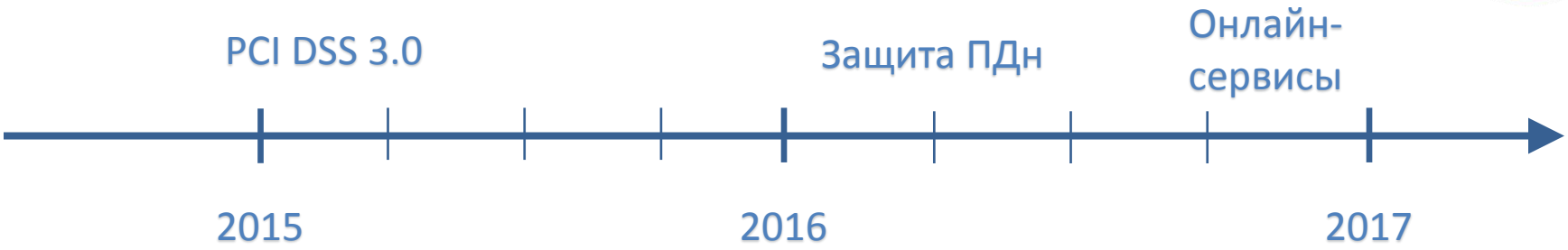
Этапность выполнения работ по сертификации облачного сервиса



Обеспечение соответствия для заказчиков

- Договор на предоставление вычислительных ресурсов облачного сервиса
- Матрица ответственности (разграничение между поставщиков услуг PCI DSS и заказчиком)
- Соглашение о конфиденциальности

Планы развития Security-as-a-Service в облачном сервисе



Сервисы ИБ	Защита ПДн	PCI DSS	Онлайн-сервисы
Межсетевое экранирование	✓	✓	✓
Обнаружение/предотвращение вторжений	✓	✓	✓
Антивирусная защита	✓	✓	
Защита виртуализации, защита от НСД	✓		
Сканирование уязвимостей	✓	✓	
Site-to-Site VPN ГОСТ	✓		
Site-to-Site VPN (AES)		✓	
Защита БД		✓	
Двухфакторная аутентификация		✓	
Контроль целостности файлов		✓	
Защита WEB-сервисов		✓	✓
Incident management (SIEM)		✓	✓

Спасибо за внимание!

Вопросы?

GO GLOBAL, GO PUBLIC, GO CLOUD, GO INNOVATIVE

Дмитрий Тирский

Департамент информационной безопасности Softline

T: +7 (495) 232 00 23 доб. 1833
M: +7 (903) 716 33 75
E-m: Dmitriy.Tirskiy@softlinegroup.com