


P2PE-сертификация платежных решений



Сергей Шустиков
Генеральный директор Deiteriy
CISA, PCI QSA (P2PE), PCI PA-QSA (P2PE)

21 июля 2016 года



Что такое PCI P2PE?

- **НОВЫЙ** стандарт индустрии платежных карт – **Point – to – Point Encryption**;
- **цель 1:** поручить защиту данных платежных карт тем, кто умеет их защищать;
- **цель 2:** перестать хотеть невозможного от тех, кто не умеет их защищать.



Условия обработки данных:



Банк (поставщик услуг эквайринга):

- есть специалисты по ИБ;
- есть требования регуляторов;
- «интуитивно» понятно, что нужно защищать инфраструктуру.

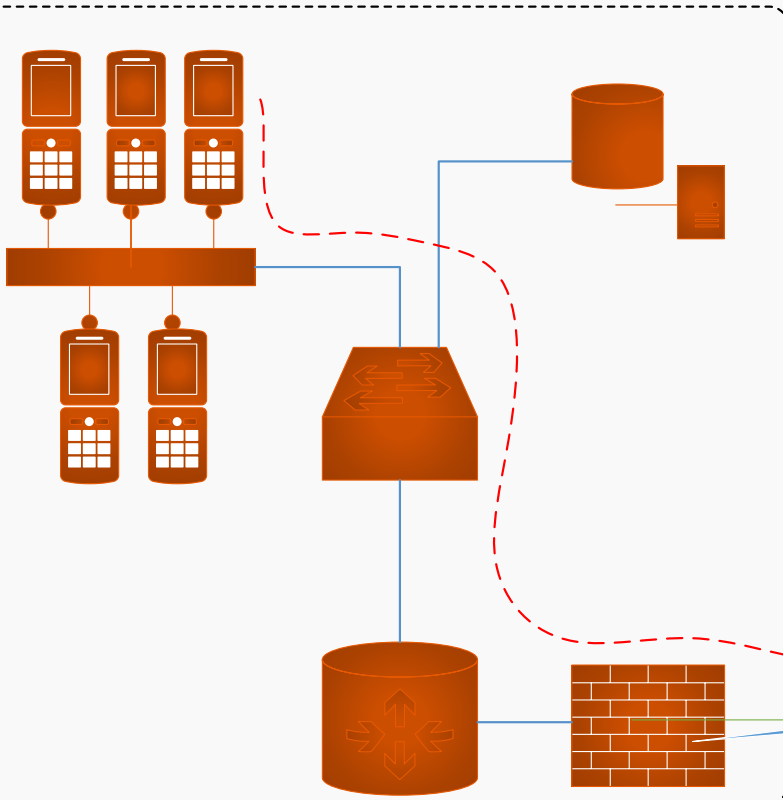
Мерчант (потребитель услуг эквайринга):

- почти нет специалистов по ИБ;
- почти нет требований регуляторов;
- «интуитивно» не является объектом для защиты данных.



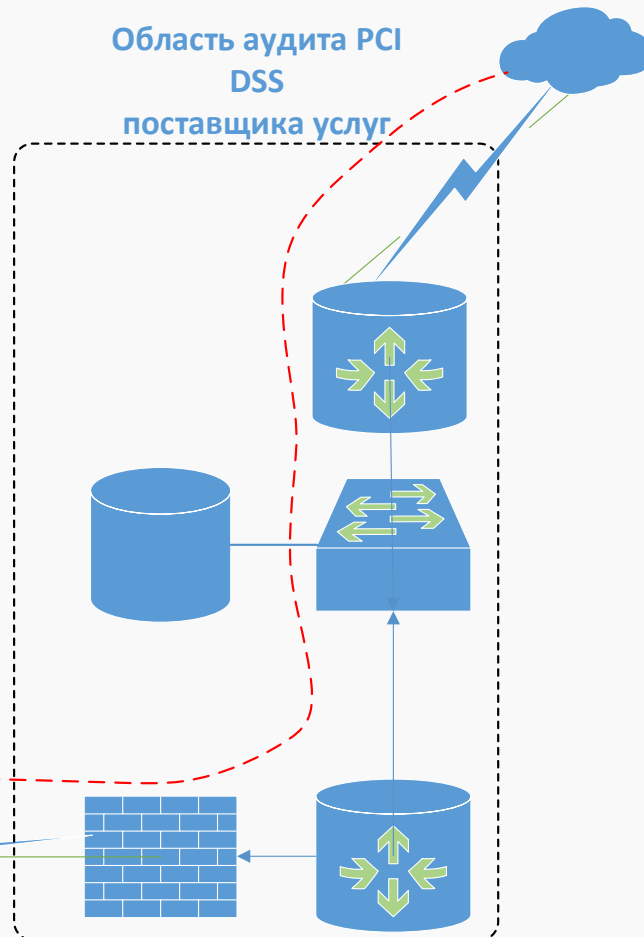


Область аудита
PCI DSS
■ мерчанта



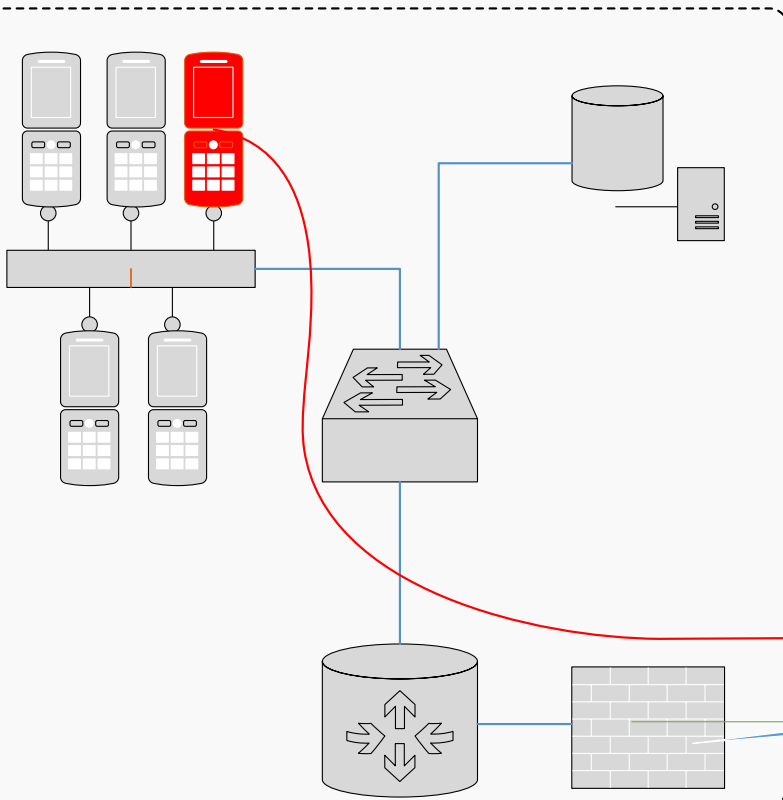
5288 36** **** 9327

Область аудита PCI
DSS
поставщика услуг



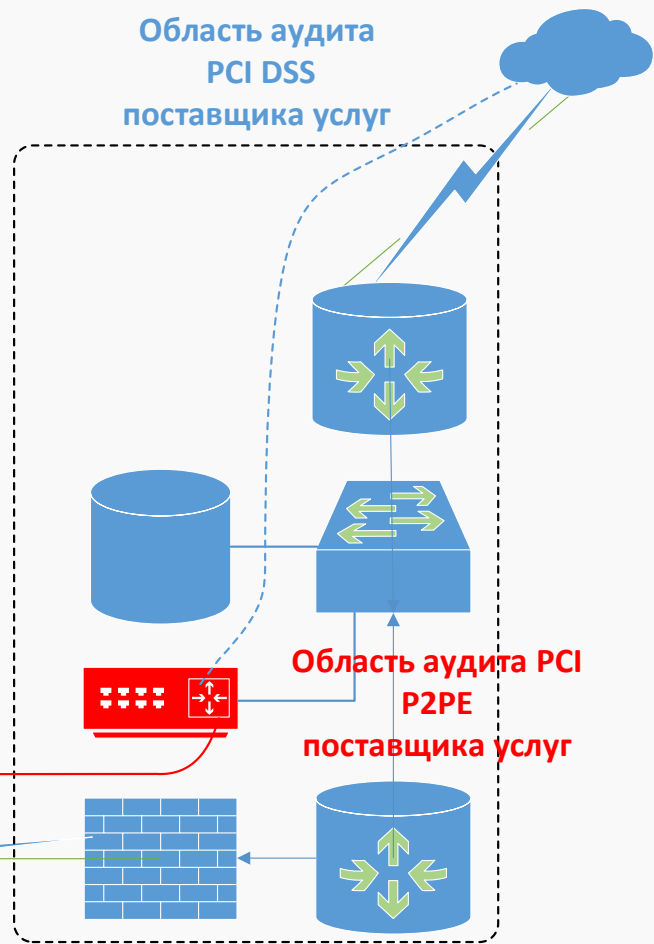


Область
самооценки SAQ
P2PE мерчанта



5288 36** **** 9327

Область аудита
PCI DSS
поставщика услуг



Область аудита PCI
P2PE
поставщика услуг



Преимущества:

- Существенное **сокращение усилий мерчанта** для соответствия PCI DSS (по сути только лист самооценки SAQ P2PE, даже для Level 1 merchant);
- Глубокий **анализ безопасности** решения на всех уровнях от физического до прикладного.



Сложности на текущий момент:

- Отсутствие внятной **документации по SRED-**функциям прошивок POS-терминалов;
- Существенно **более строгие требования** к безопасности среды расшифрования поставщика услуг P2PE.



Вопросы?

E-mail: sergey.shustikov@deiteriy.com

Facebook: [Sergey Shustikov](#)