

*V Уральский форум «Информационная безопасность банков»
11-16 февраля 2013, Республика Башкортостан*



Информзащита
Системный интегратор

Программа для банков-эквайеров по приведению мерчантов к PCI DSS

Алексей Бабенко

руководитель направления, PA&PCI QSA

О чем Вы могли забыть...

Стандарт PCI DSS применим **ко всем** объектам и организациям, осуществляющим хранение, обработку или передачу данных платежных карт.

МПС определяют требования по подтверждению соответствия и штрафные меры, исходя из собственных рисков.

Крайние сроки уже наступили (~~сентябрь 2010, март 2011, июль 2012~~).



Требования МПС

Visa Account Information Security 

www.visacemea.com/ac/ais/data_security.jsp

MasterCard Site Data Protection



www.mastercard.com/sdp

American Express Data Security



www.americanexpress.com/datasecurity

Discover Information Security & Compliance



www.discovernetwork.com/merchants/fraud-protection

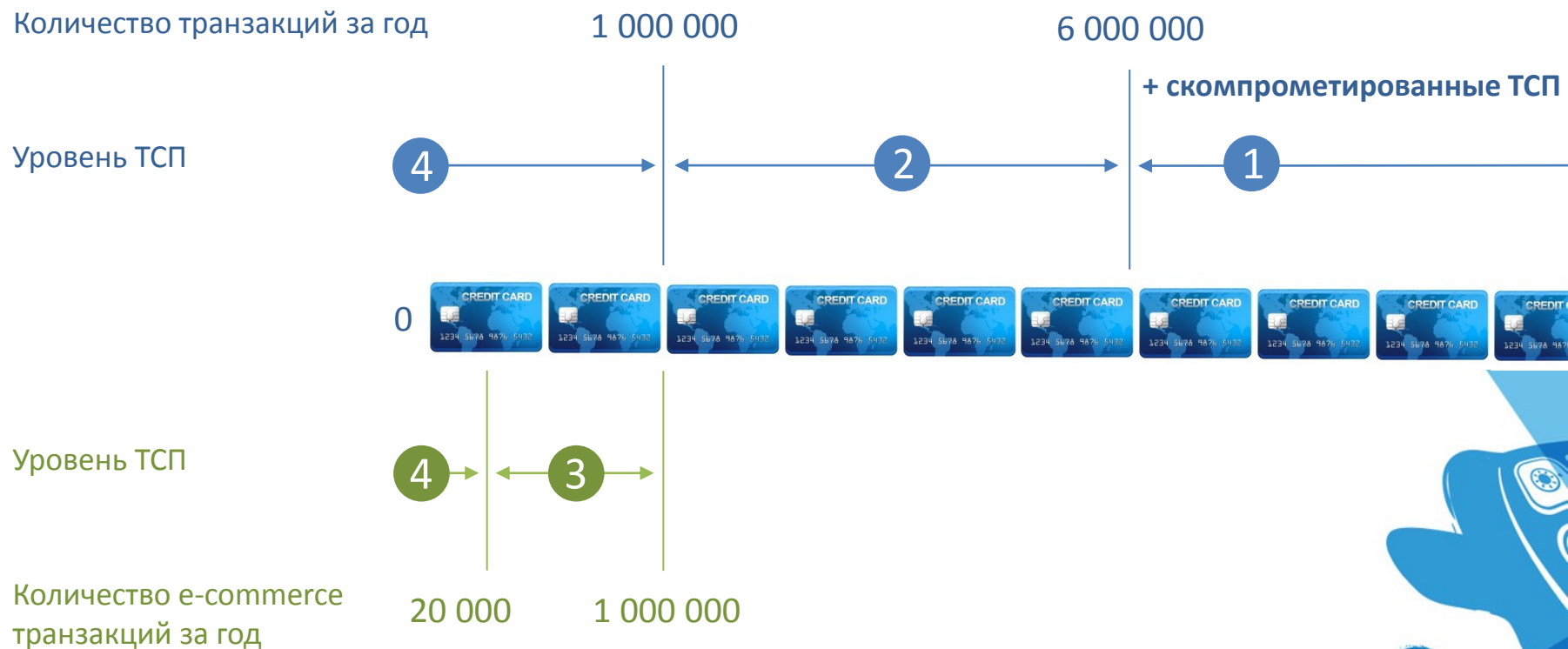
JCB Data Security Program



www.partner.jcbcard.com/security/jcbprogram



Уровни торгово-сервисных предприятий



Согласно:

Visa Account Information Security
MasterCard Site Data Protection

Подтверждение соответствия ТСП требованиям PCI DSS

1

2

3

4

 VISA



ASV

QSA



ASV

SAQ



ASV

SAQ



ASV и SAQ
по требованию

 MasterCard
Worldwide



ASV

QSA



ASV

QSA



ASV

SAQ



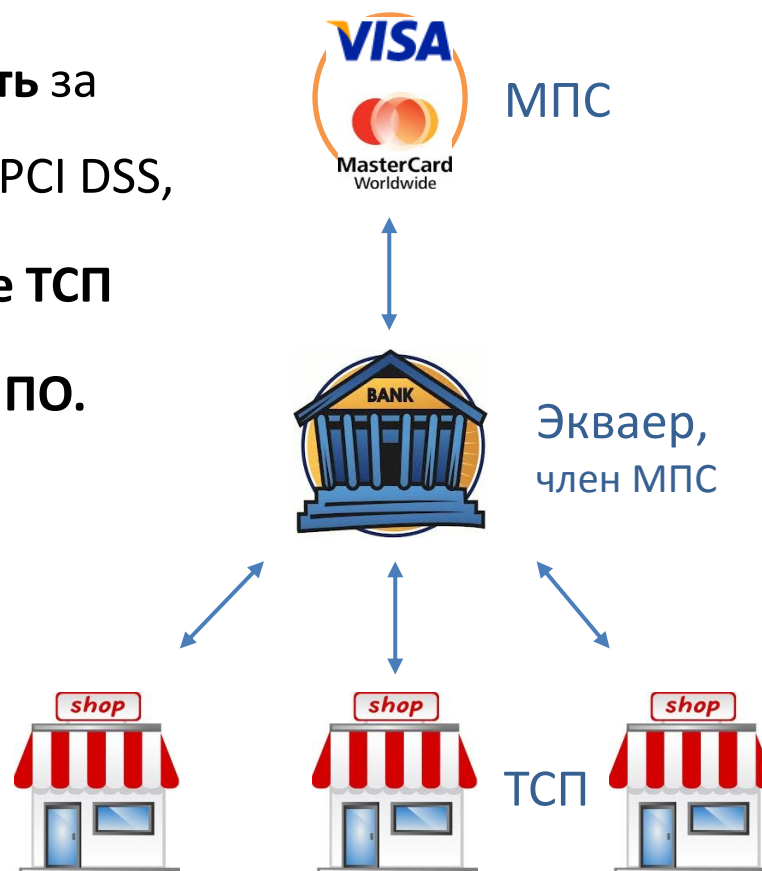
ASV

SAQ

1

Отчетность о соответствии PCI DSS

Эквайер несет ответственность за
соблюдение ТСП требований PCI DSS,
в том числе за использование ТСП
PA-DSS сертифицированного ПО.



Согласно:

Visa Account Information Security

MasterCard Site Data Protection

http://www.mastercard.com/us/merchant/pdf/SDP_Program_Revisions.pdf

<http://corporate.visa.com/media-center/press-releases/press931.jsp>

Отчетность о соответствии PCI DSS



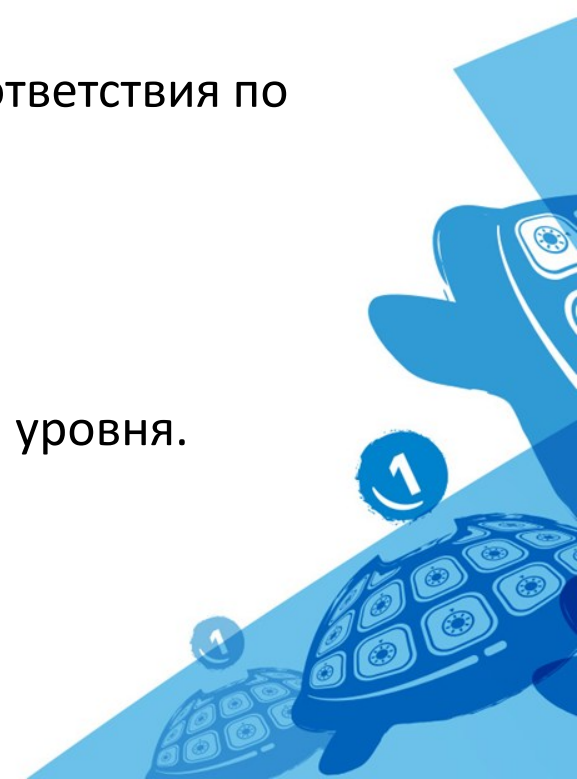
Отчетность каждые полгода:

- статус каждого ТСП 1 и 2 уровня,
- сводная статистика по ТСП 3 уровня.

МПС может запросить документацию о проверке соответствия по конкретному ТСП.



Отчетность ежеквартально: статус каждого ТСП 1, 2, 3 уровня.

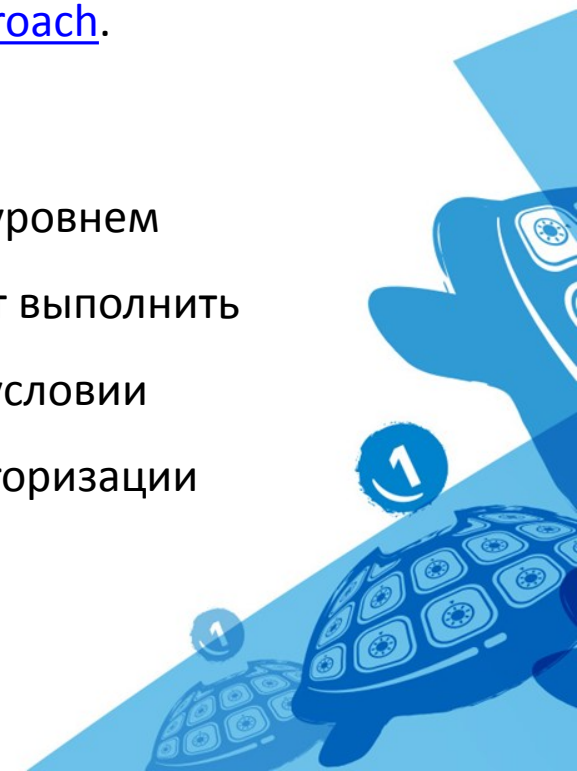


Risk-based PCI DSS Validation



ТСП реализовавшие шифрование канала передачи ДПК от точки захвата до процессинга (ТСП не имеет доступа к данным) могут выполнить только первые 4 пункта [PCI SSC's Prioritized Approach](#).

ТСП реализовавшие прием карт с EMV чипом, для стран с уровнем использования EMV-транзакций с iCVV не менее 75% могут выполнить только первые 4 пункта [PCI SSC's Prioritized Approach](#). При условии доказательства отсутствия хранения критичных данных авторизации ТСП 1 уровня могут заменить QSA-аудит заполнением SAQ.

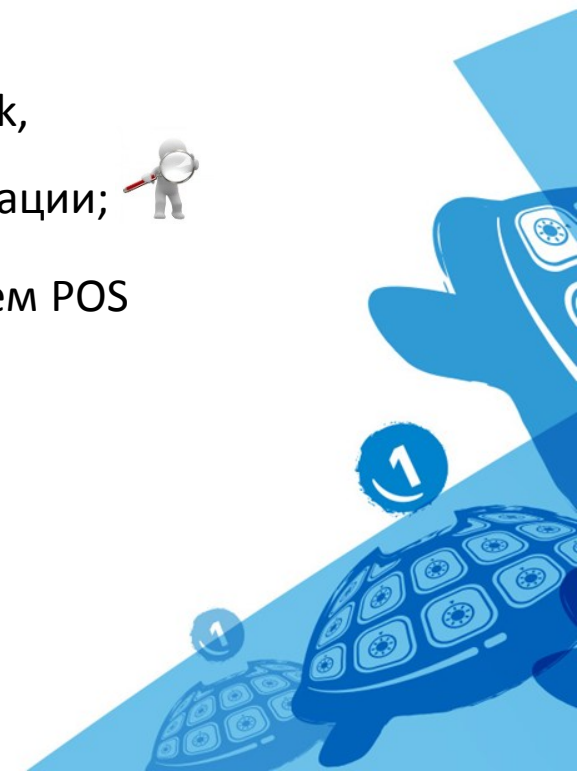


Visa Technology Innovation Program (TIP)



ТСП могут быть освобождены от ежегодной оценки, если:

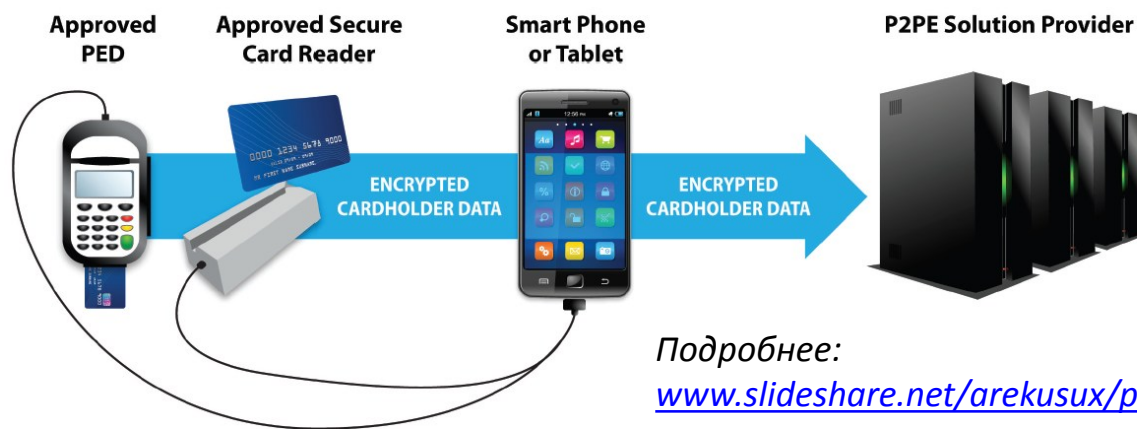
- Был подтвержденный факт соответствия PCI DSS (либо составлен план по его достижению); 
- Критичные данные авторизации (track1/2, PIN/PIN-block, CVV2) не хранятся после завершения процесса авторизации; 
- Не менее 75% транзакций обработано с использованием POS терминалов, поддерживающих EMV-транзакции/ беспроводные карты; 
- Нет прецедентов компрометации данных карт. 



P2PE (Point-to-Point Encryption) решения

Решение P2PE – совокупность устройств, ПО и процессов, обеспечивающая надежное шифрование данных платежных карт от точки взаимодействия (POI) до среды расшифрования, а именно:

- Надежное шифрование данных платежных карт в точках взаимодействия с клиентом (POI);
- Использование P2PE сертифицированных приложений в точках взаимодействия;
- Безопасное управление устройствами шифрования/расшифрования;
- Обеспечение безопасности среды расшифрования данных и самих данных в открытом виде, безопасное управление ключами.



Подробнее:

www.slideshare.net/arekusux/pci-p2pe

Выгода от внедрения P2PE решений

1

Использование P2PE решений, позволяет сократить область проверки PCI DSS для ТСП 1 уровня.

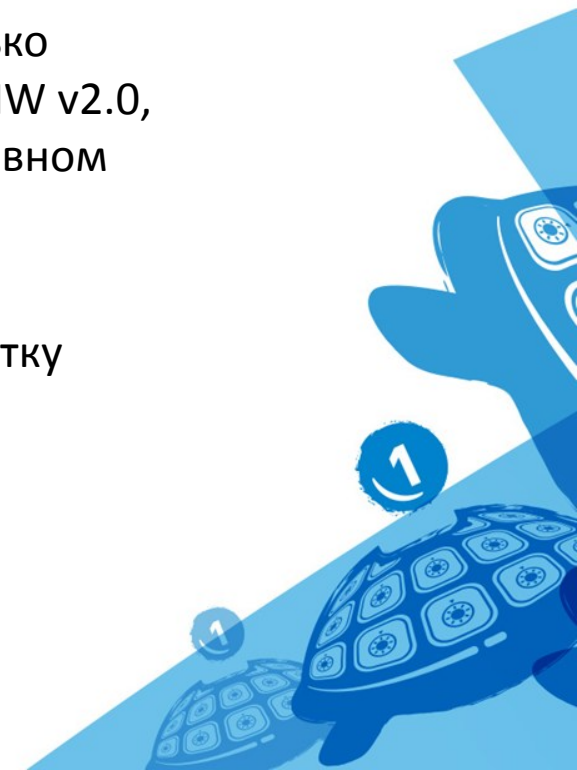
2

3

4

ТСП уровня 2-4, использующие для обработки данных только сертифицированные P2PE решения, заполняют SAQ P2PE-HW v2.0, содержащий минимальное количество требований (в основном требования к документированным политикам).

P2PE решения помогают обеспечивать безопасную обработку данных платежных карт.

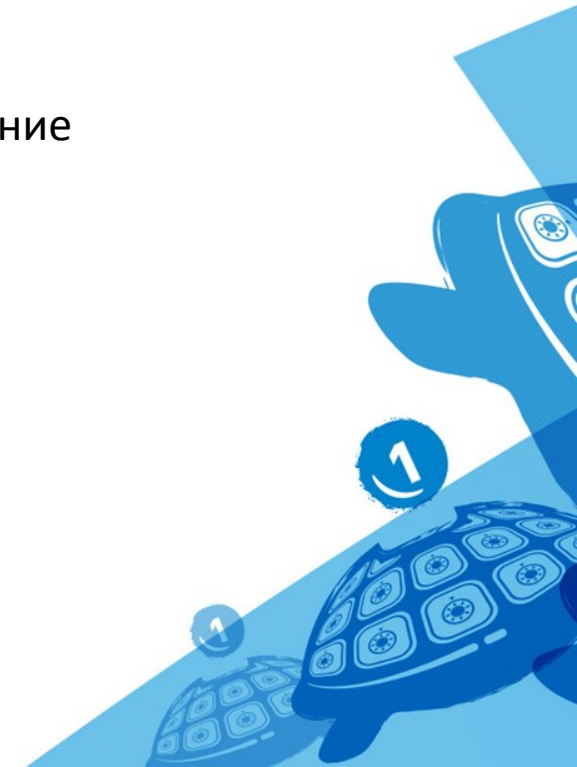


Услуги компании «Информзащита»

**Разработка программы контроля соответствия ТСП;
PCI DSS Compliance для ТСП 1 и 2 уровня;
Заполнение SAQ PCI DSS для ТСП 2, 3 и 4 уровня;
Сканирование PCI ASV.**

Подготовка , проведение сертификации PCI DSS, поддержание соответствия требованиям PCI DSS;
Тест на проникновение PCI DSS.

Сертификация и поддержание соответствия программного обеспечения требованиям стандарта PA-DSS.



Почему мы?

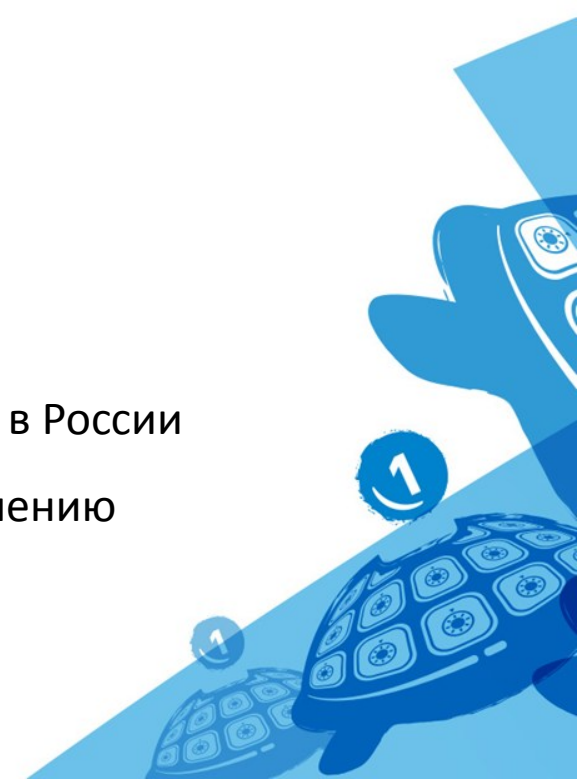
Первые в СНГ: QSA и ASV с 2006 года, PA-QSA с 2008 года.

Профессиональный штат: 8 QSA аудиторов, 2 PA-QSA аудитора.



Более 70 аудитов PCI DSS, 11 сертифицированных PA-DSS приложений.

Более 2500 государственных и коммерческих организаций в России и странах СНГ доверили нам выполнение работ по обеспечению информационной безопасности.





Информзащита
Системный интегратор

Вопросы?

Алексей Бабенко

руководитель направления, PA&PCI QSA

a.babenko@infosec.ru

+7 (495) 980-23-45 доп.458

www.infosec.ru

arekusux.blogspot.com