Какие приложения подлежат сертификации PA-DSS? Вам поможет опросник от Совета PCI SSC

В платежной индустрии существуют самые разнообразные "платежные приложения", которые мерчанты могут встраивать в среду транзакций. Хотя PA-DSS – это производственный стандарт для разработки платежных приложений, не все приложения, имеющие отношение к транзакциям, подлежат аудиту и включению в программу PA-DSS Советом PCI SSC.

В контексте PA-DSS платежное приложение, подлежащее аудиту и включению в программу Советом PCI SSC, определяется как такое приложение, которое:

а) хранит, обрабатывает или передает данные о держателях карт (ДДК) в процессе авторизации или подтверждения транзакций; и
б) продается, распространяется или передается по лицензии третьим лицам.

Следующий список вопросов поможет определить, подлежит ли данное приложение аудиту и включению в программу PA-DSS Советом PCI SSC.

В случае ответа "ДА" на ЛЮБОЙ из следующих вопросов приложение НЕ подлежит сертификации PA-DSS:

1. Это бета-версия приложения?

2. Это приложение использует данные о держателях карт, но само по себе не участвует в авторизации или подтверждении транзакций?

3. Это приложение участвует в авторизации или подтверждении транзакций, но не имеет доступа к ДДК или критичной аутентификационной информации?

4. Это приложение требует от пользователя доработки исходного кода или значительных изменений в конфигурации (в отличие от продажи и установки в готовом виде), так что изменения влияют на одно или многие требования PA-DSS?

5. Это приложение является системой личного кабинета, которая хранит ДДК, но не участвует в авторизации или подтверждении транзакций по кредитным картам? Например:

- *Отчетность и управление ресурсами компании*
- *Учет вознаграждений или нарушений*

6. Это приложение разрабатывается для личного пользования и не выйдет за пределы компании-разработчика?

7. Это приложение разрабатывается для конкретного клиента, продается только ему и будет использоваться только им?

8. Это приложение функционирует как библиотека общего доступа (например DLL), и для его работы необходима установка другого приложения, но они не продаются, лицензируются и/или распространяются единым пакетом?

9. Соответствие этого приложения требованиям PA-DSS зависит от работы другого приложения, но они не продаются, лицензируются и/или распространяются единым пакетом?

10. Это приложение – отдельный модуль, который не является неотъемлемой частью системы, а сам по себе не участвует в авторизации или подтверждении транзакций?

11. Это приложение предлагается клиентам только на условиях SaaS ("ПО как услуга"), не продается, не распространяется и не передается по лицензии третьим лицам?

12. Это приложение является операционной системой, базой данных или платформой, пусть даже такой, которая может хранить, обрабатывать или передавать ДДК?

13. Это приложение разработано для потребительских электронных портативных устройств (например, смартфонов, планшетов или КПК), функции которых не ограничиваются принятием оплаты по транзакциям?

Пожалуйста, имейте в виду, что вышеприведенный список неполон, составлен исключительно в показательных целях и может быть дополнен Советом PCI SSC в любой момент.

Что делать продавцу товаров или услуг, если он использует или намеревается использовать приложения, которые хранят, обрабатывают или передают ДДК, но не подлежат сертификации PA-DSS?

Приложения, которые хранят, обрабатывают или передают ДДК, но не подлежат сертификации PA-DSS, войдут в скоуп ежегодного аудита PCI DSS этой организации, и тогда будет проверено их соответствие всем применимым требованиям PCI DSS.

Что делать разработчику приложения, если их продукт не подлежит сертификации по программе PA-DSS Совета PCI SSC?

Если приложение не подлежит сертификации по программе PA-DSS Совета PCI SSC, тогда PCI SSC рекомендует разрабатывать такие приложения, которые предполагается использовать в среде ДДК, с учетом PA-DSS как основы защиты информации о платежных картах.

Продавцы товаров или услуг, которые используют или хотят использовать эти приложения в своей среде ДДК, должны будут включить их в скоуп своего ежегодного аудита PCI DSS.

Пожалуйста, имейте в виду, что у каждой платежной системы своя программа проверки соответствия, и в ней могут быть специфические условия использования приложений, не сертифицированных по PA-DSS, требования к отчетам, сроки прохождения аудитов, стоимость, штрафы и т.п. За информацией о специфических требованиях платежных систем к соответствию вы можете обратиться в свой банк-эквайрер или непосредственно в платежную систему.