РусКрипто

XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

Контактные и бесконтактные платежи: криптография под капотом

Никифорова Лидия Олеговна, ведущий инженер-аналитик, ООО «КРИПТО-ПРО»
Ахметзянова Лилия Руслановна, к.ф.-м.н. зам. начальника отдела криптографических исследований, ООО «КРИПТО-ПРО»
Бабуева Александра Алексеевна, к.ф.-м.н. ведущий инженер-аналитик, ООО «КРИПТО-ПРО»
Никонов Николай Владимирович, в.н.с. лаборатории НКО «Фонд содействия развитию безопасных информационных технологий»

Оплата картой – это криптографический протокол между картой (и её владельцем), терминалом и банком эмитентом

транзакция

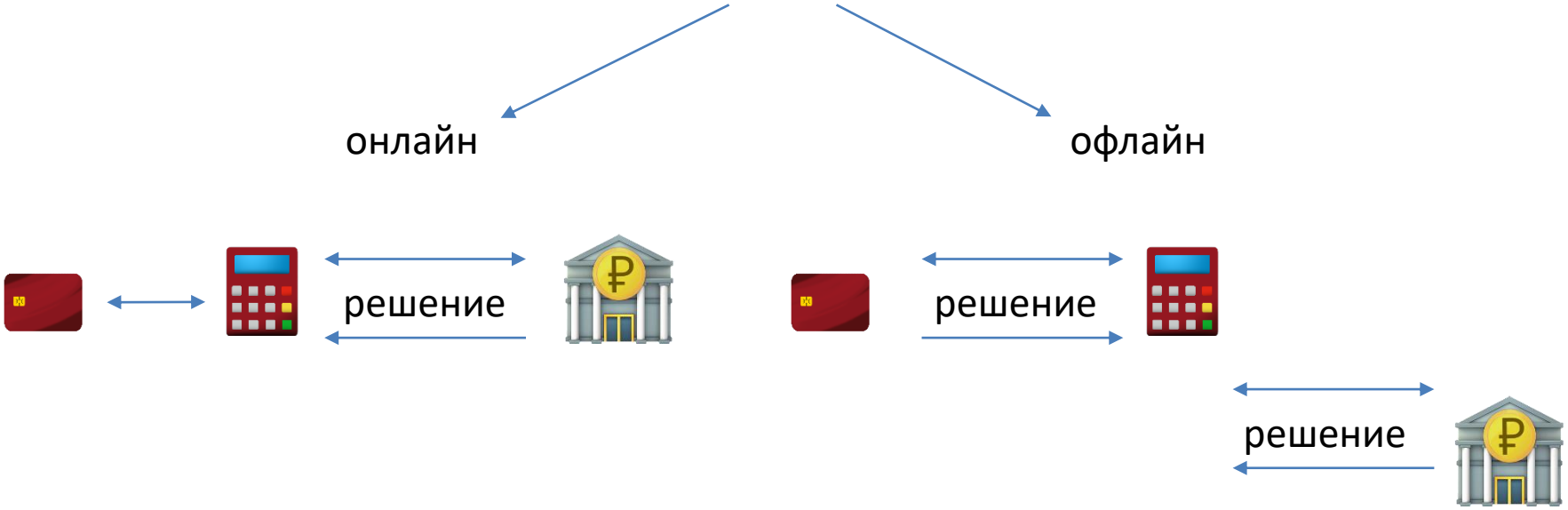
решение

решение

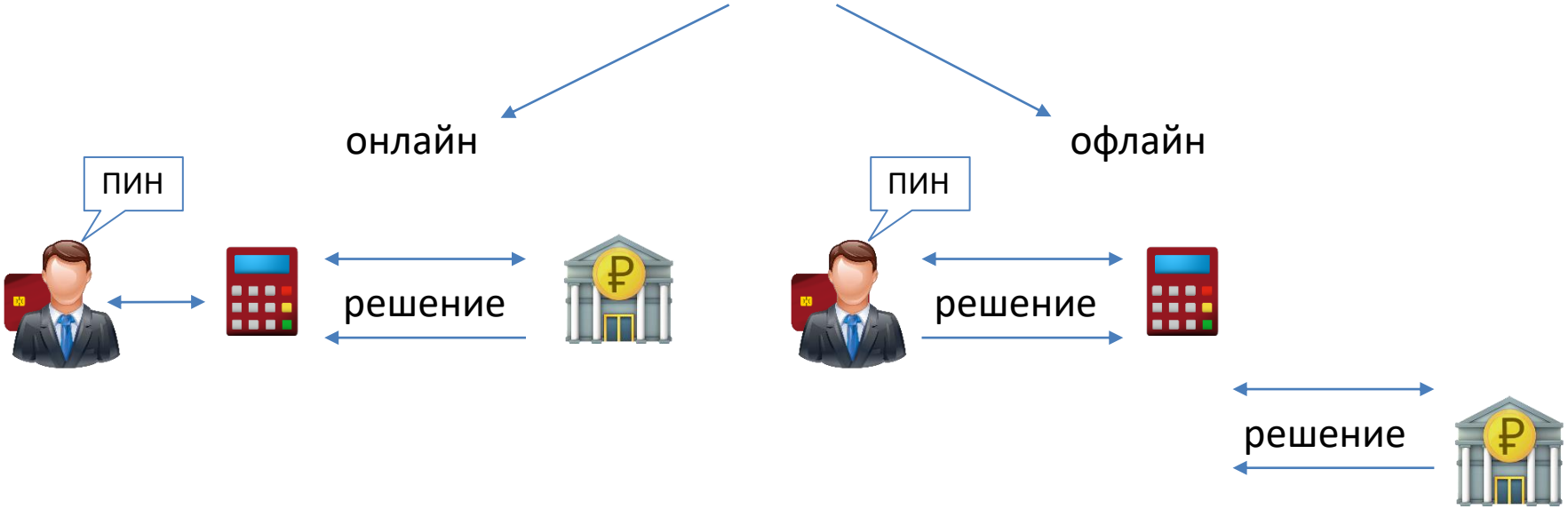
решение

Решение должно быть согласованным

Сценарии обработки транзакции



Сценарии обработки транзакции

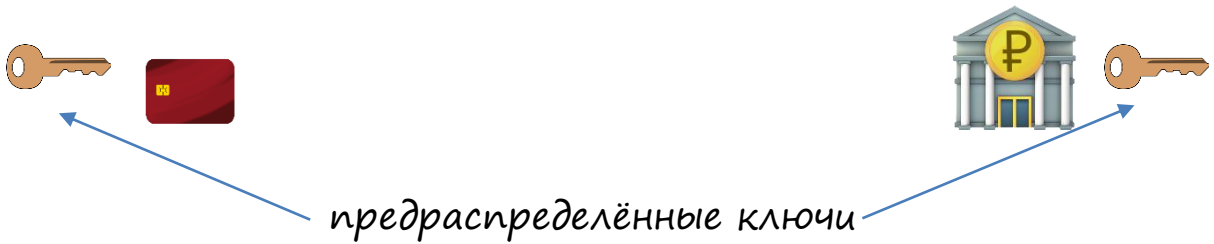


Режимы работы

контактный

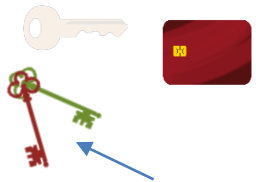
бесконтактный

Начальные условия



Между картой и эмитентом симметричная криптография

Начальные условия

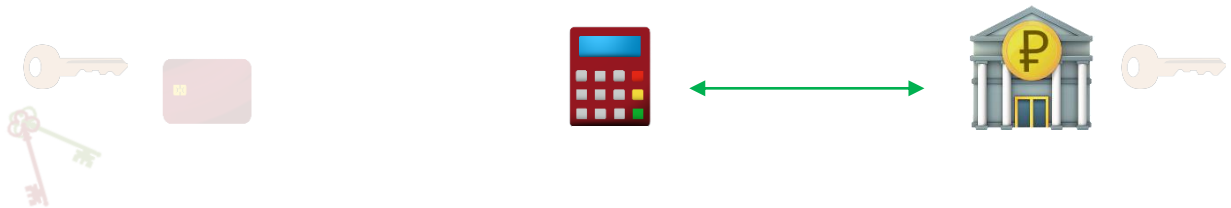


долговременная ключевая пара и сертификат

Между картой и эмитентом симметричная криптография

Между картой и терминалом асимметричная криптография

Начальные условия



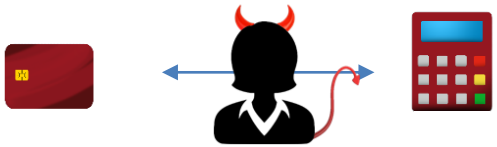
Между картой и эмитентом симметричная криптография

Между картой и терминалом асимметричная криптография

Между терминалом и эмитентом защищённый канал

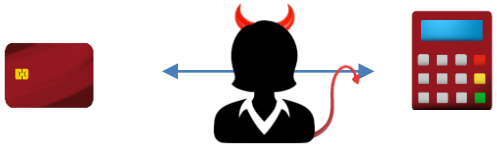
От чего должен защищать протокол?

Нарушитель может

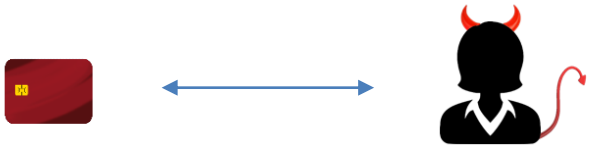


Вмешиваться в канал между картой и терминалом

Нарушитель может

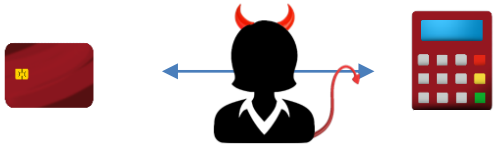


Вмешиваться в канал между картой и терминалом

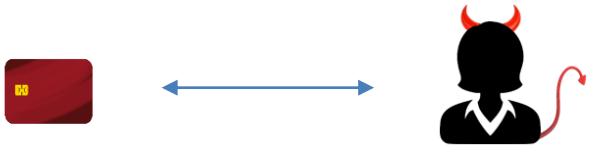


Взаимодействовать с картой от лица терминала

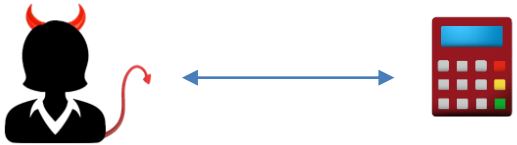
Нарушитель может



Вмешиваться в канал между картой и терминалом

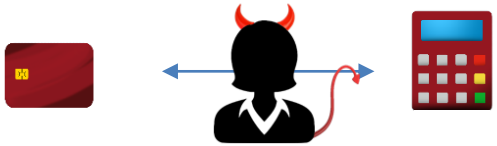


Взаимодействовать с картой от лица терминала

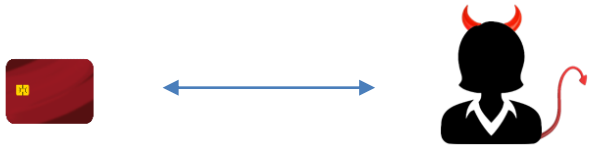


Взаимодействовать с терминалом от лица карты

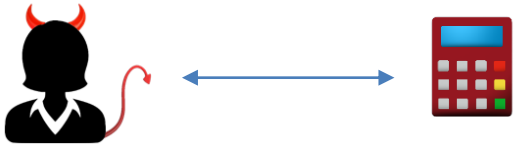
Нарушитель может



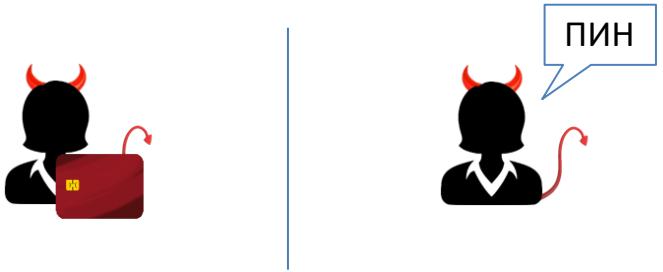
Вмешиваться в канал между картой и терминалом



Взаимодействовать с картой от лица терминала

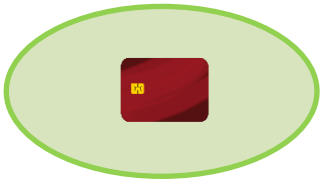


Взаимодействовать с терминалом от лица карты



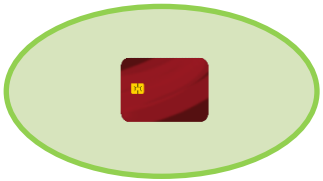
Украсть карту или узнать ПИН

Нарушитель не может

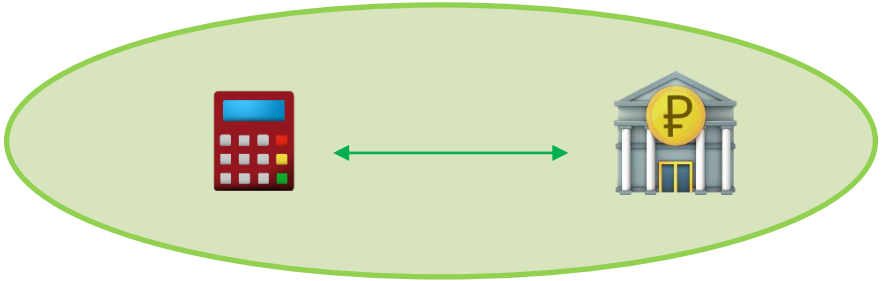


Менять логику работы карты

Нарушитель не может



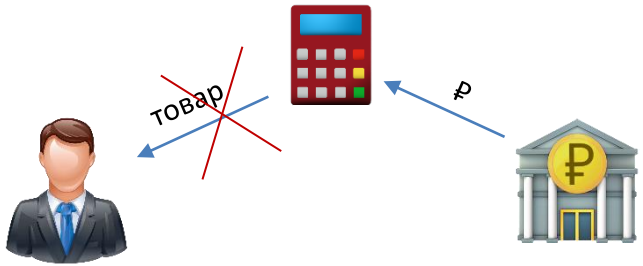
Менять логику работы карты



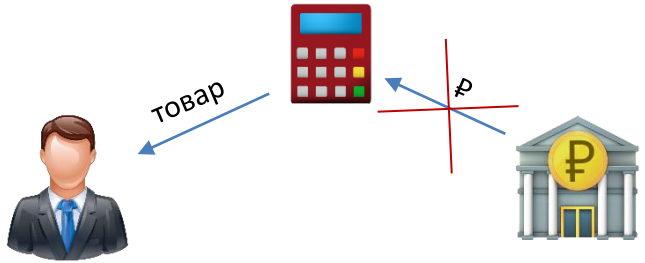
Взаимодействовать с эмитентом от лица терминала

Протокол оплаты предназначен для защиты от двух угроз:

1. Эмитент примет транзакцию, неаутентифицированную терминалом или владельцем карты



2. Терминал примет транзакцию, которая будет отклонена эмитентом



Что в платёжной системе МИР?

Угроза 1

Реализация угрозы означает, что карта или её владелец не принимали транзакцию, а эмитент принял



транзакция

Не принята

Принята

Угроза 1

$data$ – статические данные карты

$data$

Формирует tr
Генерирует случайно UN

tr, UN

$AC = MAC(SK_{AC}, data \parallel tr \parallel UN \parallel res)$

Криптограмма

AC, res

$AC, tr, UN, data, res$

$AC\ ? = MAC(SK_{AC}, data \parallel tr \parallel UN \parallel res)$

Угроза 1

$data$ – статические данные карты

$data$

Формирует tr
Генерирует случайно UN

tr, UN

$AC = MAC(SK_{AC}, data \parallel tr \parallel UN \parallel res)$

AC, res

$AC, tr, UN, data, res$

$AC \stackrel{?}{=} MAC(SK_{AC}, data \parallel tr \parallel UN \parallel res)$

Нарушителю нужно передать терминалу AC для $res = OK$, при этом владелец карты не должен соглашаться на данную транзакцию

Угроза 1

Relay атака

tr, UN

tr, UN

tr, UN

AC, res

AC, res

AC, res

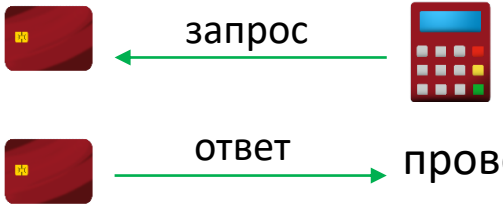
Угроза 1

Relay атака

Бесконтактный режим

Контактный режим

Есть протокол защиты:

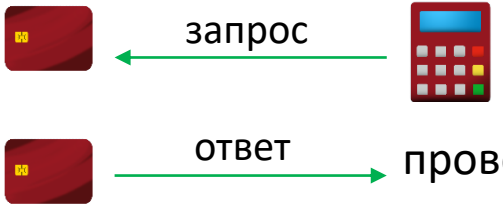


Угроза 1

Relay атака

Бесконтактный режим

Есть протокол защиты:



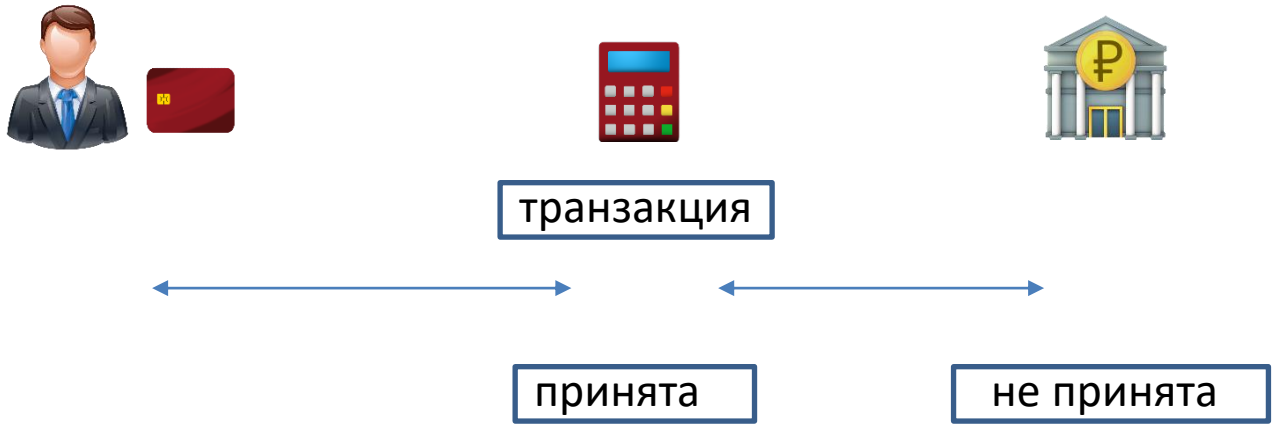
проверяет время отклика

Контактный режим

Защита за счёт размера карты

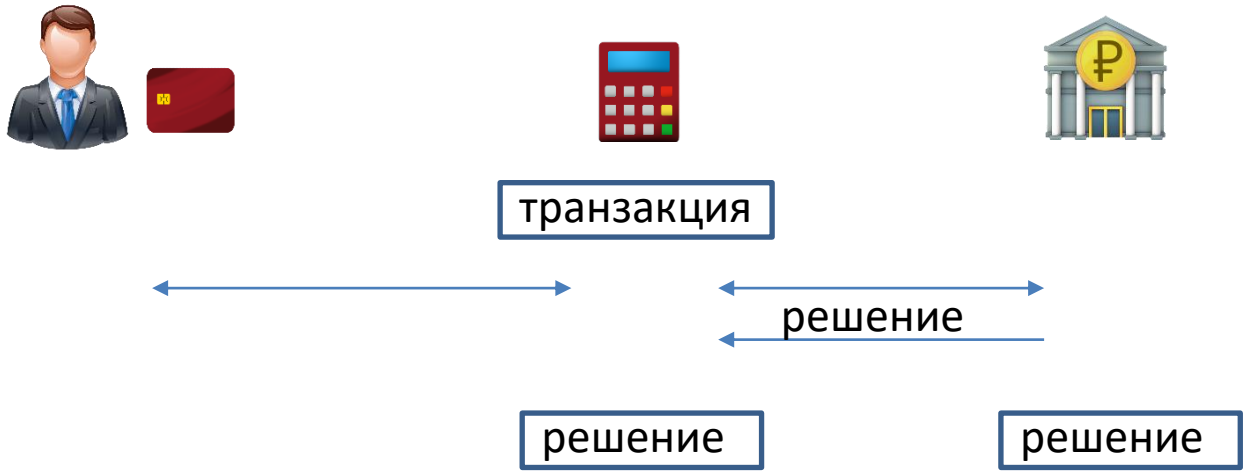
Угроза 2

Реализация угрозы означает, что терминал принял транзакцию, а эмитент отклонил

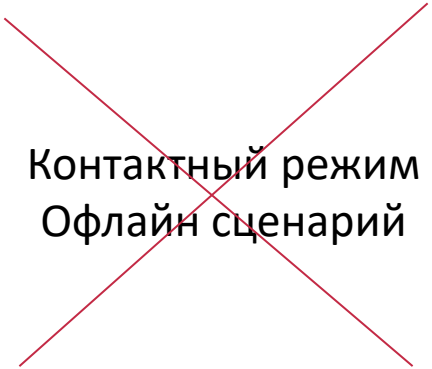


Угроза 2

Для онлайн сценария угроза не актуальна



Угроза 2



Есть только онлайн сценарий в контактном режиме

⇓

Нет асимметричной криптографии в контактном режиме

Угроза 2

В офлайн сценарии терминал должен убедиться, что данные прислала карта

Угроза 2

В офлайн сценарии терминал должен убедиться, что данные прислала карта

Бесконтактный режим: выполняется установление защищённого канала

Угроза 2

Q_k

Генерирует ключевую пару (d_k, Q_k)

Генерирует случайную маску α

Вычисляет общий секрет $K = \alpha \cdot d_c \cdot Q_k$

Вычисляет маскированный открытый ключ $Q'_c = \alpha \cdot Q_c$

Вычисляет сессионные ключи K_{enc}, K_{mac}

Зашифровывает маску $\alpha' = Enc(K_{enc}, \alpha)$

Q'_c, α'

Вычисляет общий секрет $K = d_k \cdot Q'_c$

Вычисляет сессионные ключи K_{enc}, K_{mac}

Расшифровывает маску $\alpha = Dec(K_{enc}, \alpha')$

Снимает маску с Q'_c, узнаёт Q_c

...

$Enc(K_{enc}, cert)$

Проверяет, что сертификат для Q_c, аутентифицирует карту

Угроза 2

Q_k

Генерирует ключевую пару (d_k, Q_k)

Генерирует случайную маску α

Вычисляет общий секрет $K = \alpha \cdot d_c \cdot Q_k$

Вычисляет маскированный открытый ключ $Q'_c = \alpha \cdot Q_c$

Ключ разный в разных сессиях
Каждая из сторон «добавляет» случайность

Вычисляет сессионные ключи K_{enc}, K_{mac}

Зашифровывает маску $\alpha' = Enc(K_{enc}, \alpha)$

Q'_c, α'

Вычисляет общий секрет $K = d_k \cdot Q'_c$

Вычисляет сессионные ключи K_{enc}, K_{mac}

Расшифровывает маску $\alpha = Dec(K_{enc}, \alpha')$

Снимает маску с Q'_c, узнаёт Q_c

...

$Enc(K_{enc}, cert)$

Проверяет, что сертификат для Q_c, аутентифицирует карту

Угроза 2

Q_k

Генерирует ключевую пару (d_k, Q_k)

Генерирует случайную маску α

Вычисляет общий секрет $K = \alpha \cdot d_c \cdot Q_k$

Вычисляет маскированный открытый ключ $Q'_c = \alpha \cdot Q_c$

Вычисляет сессионные ключи K_{enc}, K_{mac}

Зашифровывает маску $\alpha' = Enc(K_{enc}, \alpha)$

Q'_c, α'

Вычисляет общий секрет $K = d_k \cdot Q'_c$

Вычисляет сессионные ключи K_{enc}, K_{mac}

Расшифровывает маску $\alpha = Dec(K_{enc}, \alpha')$

Снимает маску с Q'_c, узнаёт Q_c

Обеспечивается анонимность карты относительно внешнего наблюдателя

...

$Enc(K_{enc}, cert)$

Проверяет, что сертификат для Q_c, аутентифицирует карту

Угроза 2

Сессионный ключ K_{mac}   Сессионный ключ K_{mac}

$MAC(K_{mac}, \text{данные карты} \parallel \text{данные транзакции}, \text{решение по транзации}, AC)$

Обеспечивается целостность данных карты, данных транзакции, решения карты по транзакции, криптограммы карты для эмитента

Контактный режим

Какие у тебя настройки?

Настройки, адреса данных

Хочу считать данные

Данные

Данные по транзакции, UN

Криптограмма

Данные карты

Данные по транзакции, UN

Криптограмма

ПИН-код*

Решение

решение

решение

Бесконтактный режим
Онлайн сценарий

Какие у тебя настройки?
Вот мой ключ

Настройки, адреса данных.
Вот мой маскированный ключ,
зашифрованная маска

Хочу считать данные

Данные (сертификат)

Данные по транзакции, UN

Криптограмма,
имитовставка для терминала

Данные карты
Данные по транзакции, UN
Криптограмма
ПИН-код*

Решение

решение

решение

Бесконтактный режим
Офлайн сценарий

Какие у тебя настройки?
Вот мой ключ

Настройки, адреса данных.
Вот мой маскированный ключ,
зашифрованная маска

Хочу считать данные

Данные (сертификат)

Данные по транзакции, UN

Криптограмма,
имитовставка для терминала

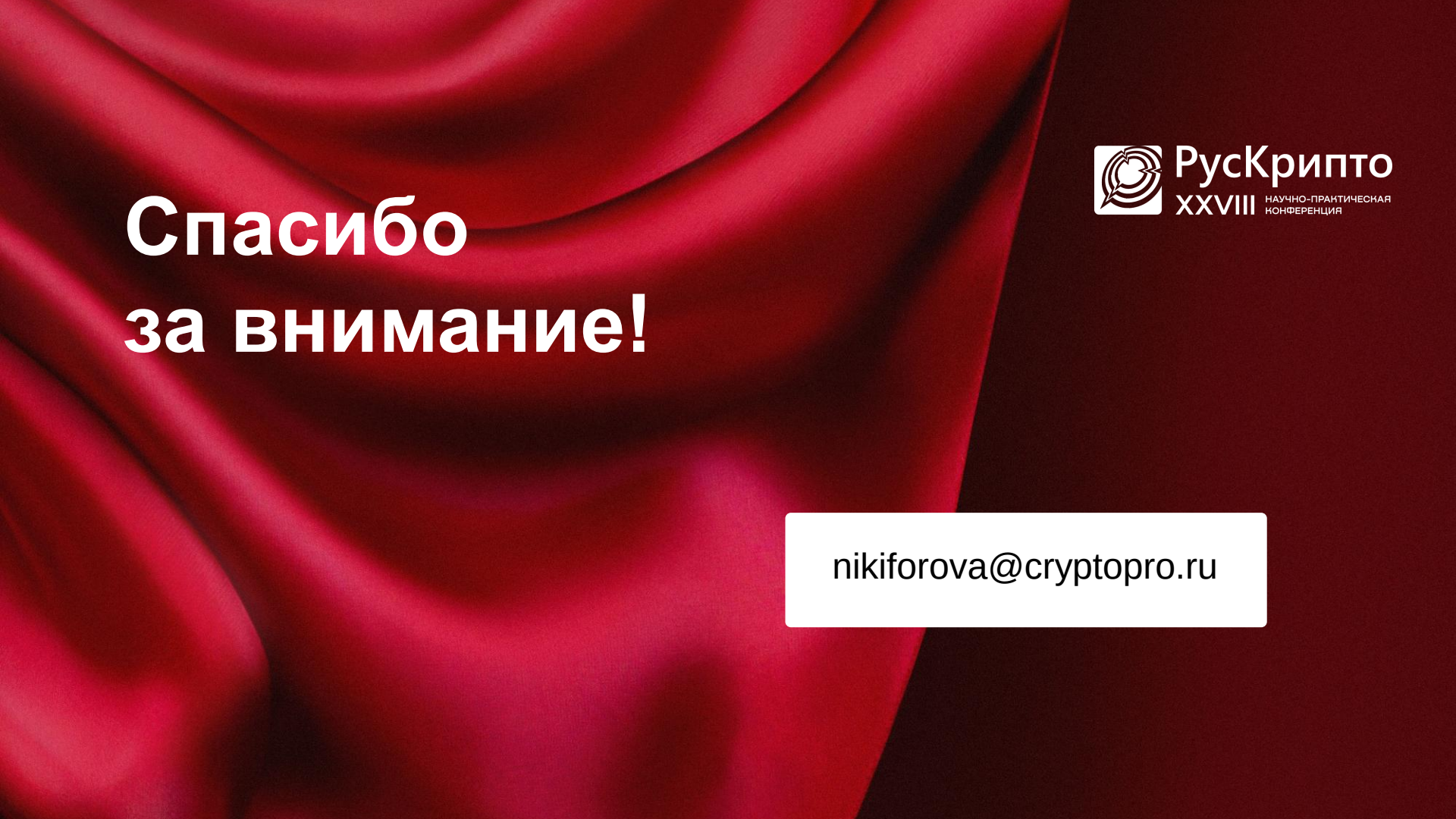
Транзакции, требующие проверки ПИН, не могут выполняться офлайн

решение

решение

Данные карты
Данные по транзакции, UN
Криптограмма

Решение


РусКрипто
XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ
Спасибо
за внимание!
nikiforova@cryptopro.ru