Система криптографической защиты CityNet System V.3.

Введение.

Программное обеспечение CityNet SV.3 используется для передачи данных между периферийными устройствами и процессинговым центром банка. Для криптографической защиты передаваемой информации используются алгоритмы 3DES. Криптографически защищается весь обмен данными между клиентским узлом CityNet SV.3, установленным в торговой точке, и серверным узлом CityNet SV.3, установленным в процессинговом центре банка.

Использование алгоритма 3DES рекомендовано международными платежными системами VISA и Eurocard-Mastercard для защиты информации о транзакциях по пластиковым картам. Основной метод защиты информации: шифрование и имитозащита данных в соответствии алгоритмом 3DES с использованием сессионных ключей шифрования.

Модуль безопасности узла CityNet SV.3

Каждый узел CityNet SV.3 содержит Модуль Безопасности (МБ), в функции которого входит хранение секретных ключей, проведение процедуры защищенной аутентификации, генерация сессионных ключей, проведение процедуры защищенной смены секретных ключей. МБ серверных узлов CityNet SV.3 реализован на базе USB-ключа или Смарт-карты e-Token. В клиентских узлах MicroSV.3 используется МБ на базе Смарт-карты ACOS-2.

МБ хранит в защищенной памяти набор ключей, которые не могут быть считаны:

- Транспортный ключ. Используется в процедуре защищенной аутентификации и генерации сессионных ключей. Может быть изменен.
- Мастер-ключ. Используется для процедуры защищенной смены Транспортного ключа. Не может быть изменен. Записывается в МБ при его инициализации.

Длина всех используемых ключей 192 бита в соответствие со стандартом шифрования 3DES.

Процедура аутентификации клиентского и серверного узлов CityNet SV.3.

При включении клиентского узла он пытается соединиться с заданным серверным узлом и провести процедуру защищенной аутентификации с выработкой сессионного ключа. Для взаимной аутентификации используется симметричная схема Challenge-Response. Пакет Challenge содержит идентификатор клиентского узла и случайную синхропосылку, выработанную МБ. Пакет Response – зашифрованный на Транспортном ключе пакет Challenge + предложенное случайное значение сессионного ключа. Выработка синхропосылки, сессионного ключа и шифрование Транспортным ключом происходят в МБ. Процедура аутентификации считается завершенной успешно, если оба узла смогли корректно расшифровать пакеты Response, что проверяется полученным значением синхропосылки.

Защищенный обмен данными.

После взаимной аутентификации клиентского и серверного узлов они переходят в режим обмена данными. Данные между узлами передаются исключительно в виде шифрограмм. Каждая шифрограмма содержит случайный вектор инициализации (8байт) выработанный в МБ, имитовставку и блок данных, зашифрованный алгоритмом 3DES на сессионном ключе. Смена сессионного ключа происходит после каждого разрыва соединения между клиентским и серверным узлом, но не реже одного раза в сутки.

Процедура смены Транспортного ключа.

Процедура смены Транспортного ключа производится в соответствие с регламентом не реже 1 раза в месяц. Новый транспортный ключ клиентского узла генерируется программным обеспечением Управления Ключами. ПО Управления Ключами шифрует новый Транспортный ключ на Мастер - ключе соответствующего клиентского узла. Используется алгоритм 3DES со случайным вектором инициализации и защитой при помощи имитовставки. Ключ в зашифрованном виде передается в серверный узел CityNet SV.3 на любом носителе. При очередной аутентификации клиентского узла ему передается сигнал о необходимости замены транспортного ключа и шифропакет с ключом. МБ клиентского узла расшифровывает пакет на Мастер - ключе, проверяет имитовставку и в случае успеха меняет значение Транспортного ключа в своей защищенной памяти. После этого заново проводится процедура аутентификации с серверным узлом уже на новых Транспортных ключах.

Программное обеспечение Управления Ключами.

ПО Управления Ключами предназначено для выработки и учета криптографических ключей, загрузки выработанных ключей на МБ, передачи ключей на серверные узлы CityNet SV.3 в зашифрованном виде и обеспечения возможности смены криптографических ключей шифрования в МБ клиентских узлов CityNet SV.3.

ПО Управления Ключами работает с локальной Базой Данных ключей. Вся информация в Базе Данных зашифрована алгоритмом 3DES на ключе эмитента. Ключ эмитента генерируется случайным образом из 3 компонент при инициализации системы. Три компоненты, используемые для генерации ключа, вводятся по отдельности тремя независимыми Уполномоченными Офицерами Безопасности.

ПО установлено на ПК, не имеющем подключений к сети и хранящемся в защищенном помещении. Доступ к работе ПО имеют только Администраторы Безопасности зарегистрированные в системе на основе персонального модуля безопасности ПМБ на базе USB-ключа e-Token Pro. После проведения аутентификации Администратор Безопасности получает возможность:

- регистрации нового узла CityNet SV.3 в Базе Данных с выработкой Мастер – ключа и Транспортного ключа с первоначальной записью их в МБ клиентского узла.
- смены Транспортного ключа узла CityNet SV.3 с генерацией файла с шифропакетом для передачи на серверный узел CityNet SV.3.
- удаление узла из Базы Данных.