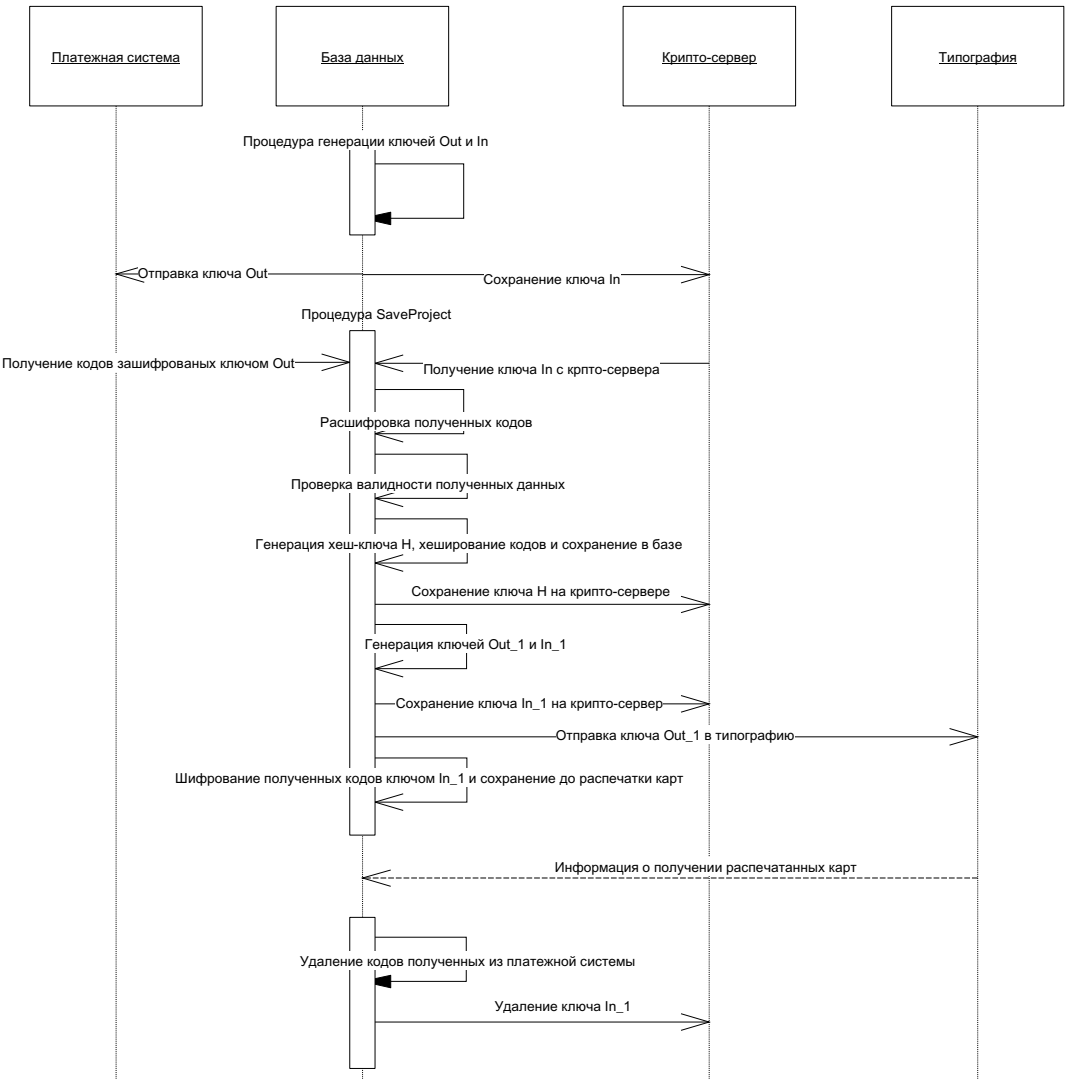
Получение кодов из платежной системы



Весь процесс обработки происходит по аккаутном администратора. База данных и крипто-сервер находятся в одном домене, поэтому права для генерации ключей, сохранения их на крипто-сервере, получение даннах для выгрузки в типографию, генерация хэш-ключа и сохранение его на крипто-сервере, отслеживаются на доменном уровне.
1. На первом шаге генерируется пара ключей, приватный и внешний для конкретного проекта. Внешний отсылается в платежну систему -внутренний сохраняется на крипто-сервере.
Итого:
В базе данных по ключам нет.

2. Получаем pin-коды от платежной системы, и запускаем процедуру SaveProject(). Права на запуск процедуры имеет администратор, поэтому процедура от имени администратора, в автоматическом режиме получает внутренний ключ, с его помощью расшифровывает данные и проверяет их валидность.
2.1 Генерируется ключ хеширования для данного проекта, pin-коды хешируются и сохраняются в таблице. Хеш-ключ передается на крипто-сервер.
2.2. Расшифрованные пин-коды вторично шифруются, с помщью заново сгенерированных внешнего и внутреннего ключа, предназначенных для типографии. (Можно было бы использовать и пару ключей из платежной системы, но тогда при утечке информации не возможно будет определить, кто ее слил).
Итого:
Данные по пин-кодам зашифрованы хешем, хеш - на крипто-сервере.
Пин коды полученные из платежной системы перешифрованны другим ключом, ключ лежит на крипто-сервере.
Данные в открытом виде доступны только в операционной памяти сервера на время исполнения процедуры, т.е. судя по объем данных и операциям над ними наверно порядка миллисекунд.
В постоянном хранении только зашифрованные данные, ключи - на другом физическом носителе.

Вместо крипто-сервера можно использовать флешку, но тогда ключи нужно будет копировать для операторов и администраторов на разные флешки, что приведет к снижению безопасности, поскольку флешку можно и в кармане унести :)