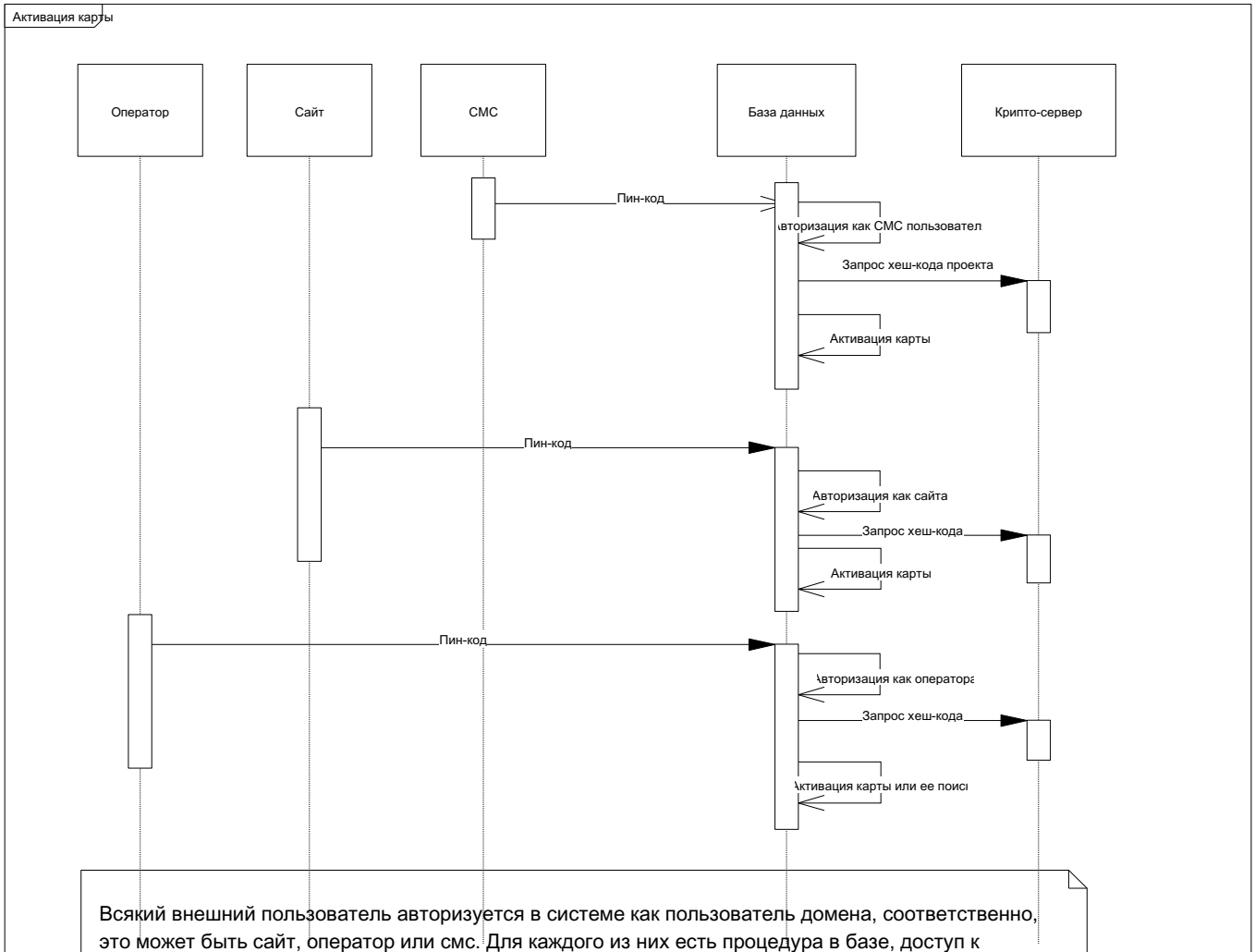

Всякий внешний пользователь авторизуется в системе как пользователь домена, соответственно, это может быть сайт, оператор или смс. Для каждого из них есть процедура в базе, доступ к которой регулируется политикой безопасности сервера и домена windows.

По результатам проверки база данных сама, без участия пользователя, по результатам авторизации, запрашивает ключ для расшифровки хеша у крипто-сервера. Таким образом, пользователь не имеет на руках ключей и не может получить к ним доступ, поскольку у него права только на запуск разрешенной ему процедуры.

Ключи на серер баз данных попадают только на время выполнения процедуры, находятся в оперативной памяти порядка миллисекунд. Передаются внутри домена windows по каналам, которые, как я понимаю, поддерживают Kerberos, с предварительным договором, шифрованием двойным ключом и прочими прелестями.