Банк Москвы

# РЕШЕНИЯ ПО БЕЗОПАСНОСТИ ДЛЯ МОБИЛЬНОГО БАНКА

Александр Ефремов

ноябрь 2015

# Требования к системе аутентификации

Банк Москвы

| Бизнес-требования | Функциональные требования | Техническое решение |
|---|---|---|
| **Удобство** : | • Отсутствие дополнительных аутентификационных устройств.<br>• Отсутствие необходимости вводить одноразовые пароли, получаемые по SMS или E-mail<br>• При аутентификации и подтверждении реквизитов транзакции Пользователь предъявляет только известный ему пароль (Passcode). | • Аутентификационные данные генерируются на стороне клиента непосредственно аутентификационным приложением в мобильном устройстве |
| **Массовость.**. | • Решение должно охватывать массовый сегмент клиентов Банка, работать на всех типах мобильных устройств<br>• Мобильное приложение устанавливается через официальные магазины: GooglePlay, AppStore, Windows Store.<br>. | • Удаленная регистрация и персонализация аутентификационного приложения<br>• Ключи и учетные данные должны храниться в памяти мобильного устройства в программном криптоконтейнере. В настоящее время невозможно обеспечивать массовое использование защищенных элементов мобильных устройств (SIM, microSD, embedded SE) для хранения ключевых и учетных данных, например PIN. |

# Требования к систем аутентификации

Банк Москвы

| Бизнес-требования | Функциональные требования | Техническое решение |
|---|---|---|
| Универсальность | • Независимость от поставщиков аутентификационных решений<br>• Возможность использования в качестве аутентификационного сервиса для единой платформы дистанционного банковского обслуживания<br>• Поддержка средств аутентификации различных вендоров: мобильные устройства, дисплейные банковские карты, CAP ридеры для банковских карт | • использование отраслевых стандартов международных платежных систем<br>• аутентификационные данные представляются в формате EMV CAP. |
| **Безопасность** . | • Должен быть обеспечен повышенный уровень безопасности для предоставления максимального спектра услуг по каналу мобильного банка.<br>• Замена канала передачи аутентификационных данных по SMS и протокола SSL<br>• Пароль пользователя не должен храниться на мобильном устройстве и хосте банка | • 2-х факторная аутентификация.<br>• Аутентификационные данные (OTP) генерируются приложением пользователя в мобильном устройстве или в банковской карте с использованием пароля и ключа аутентификационного приложения.<br>• Ключ аутентификационного приложения хранится в зашифрованном виде с использованием пароля и уникального идентификатора мобильного устройства. Пароль в памяти устройства не должен храниться.<br>• Для передачи аутентификационной информации между Банком и аутентификационным приложением устанавливается защищенное сессионное соединение |

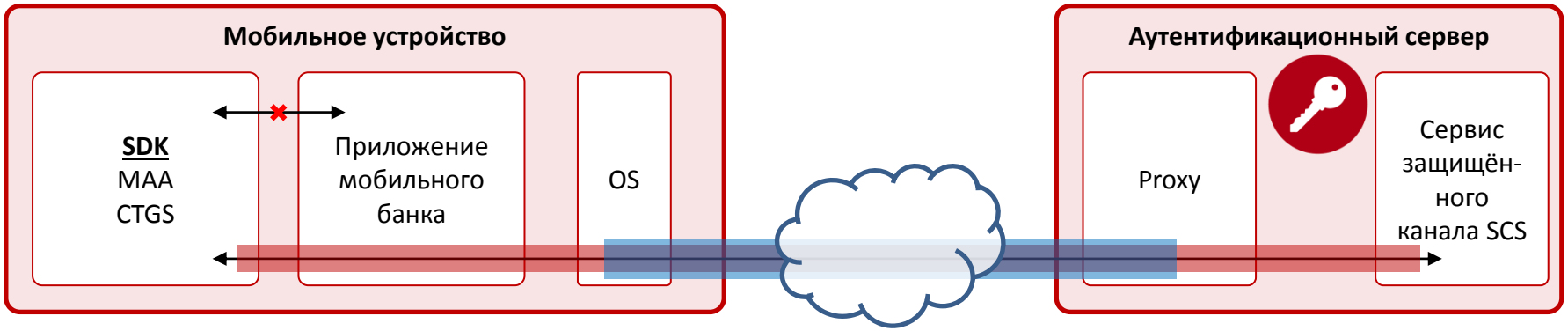
# Система аутентификации

Банк Москвы

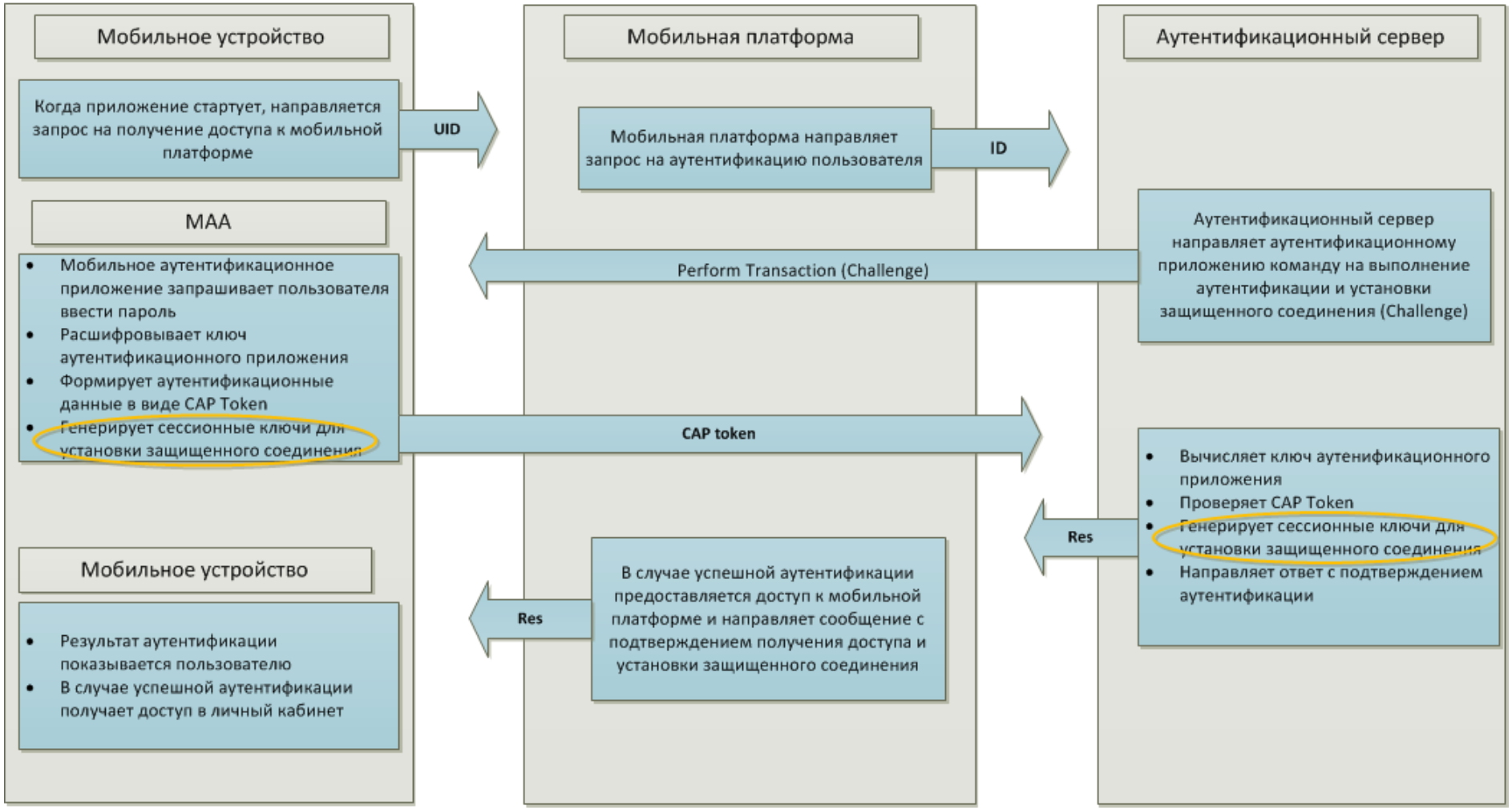
## 1. Аутентификационное приложение банковской карты переносится на мобильное устройство

| 2-х факторная аутентификация | Модель аутентификации с использованием приложения на банковской карте | Модель аутентификации с использованием приложения на мобильном устройстве |
|---|---|---|
| Что я имею |  |  |
| Что я знаю | PIN | Passcode |

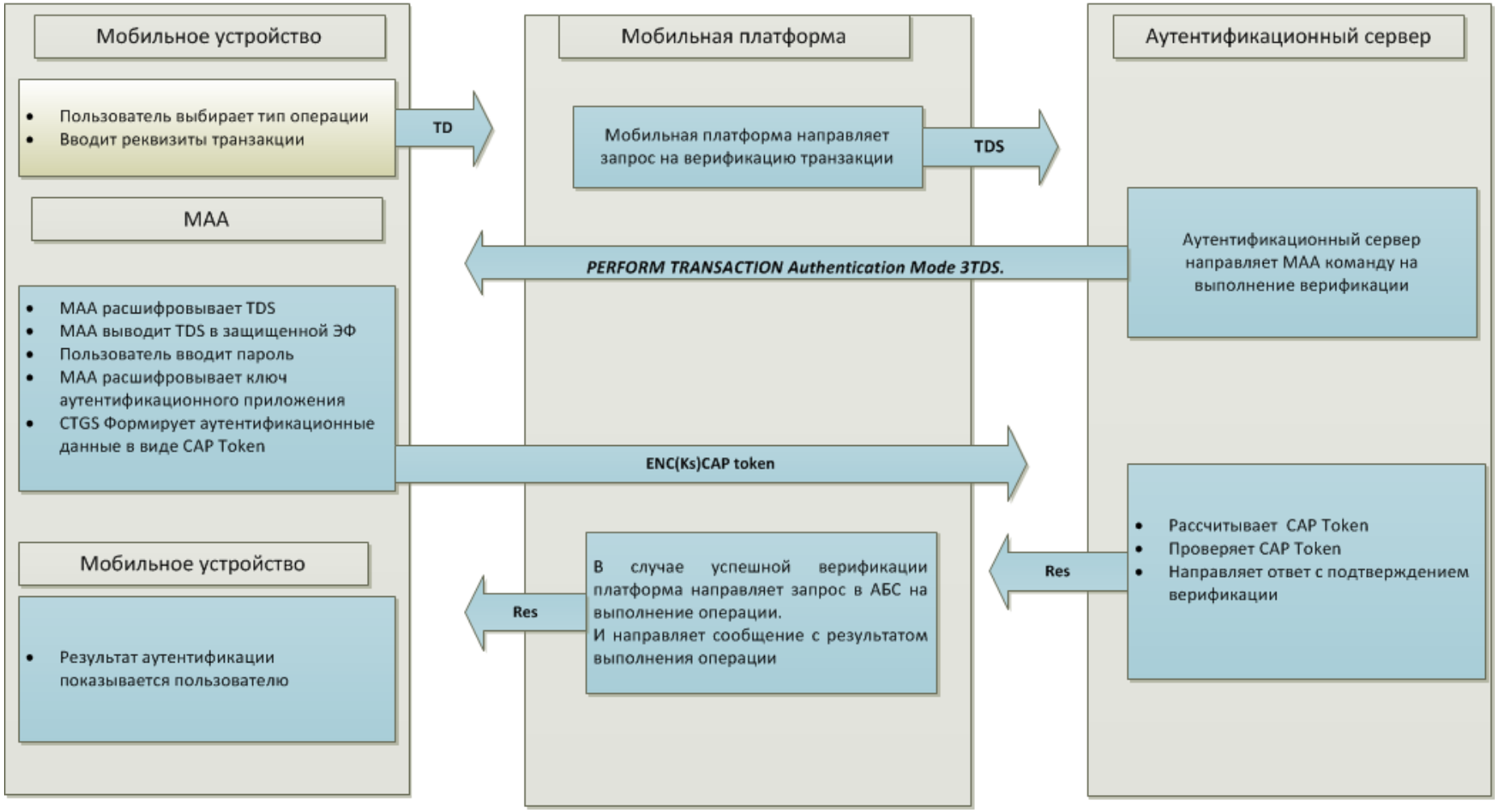
## 2. Вместо канала SSL устанавливается защищенный канал между Банком и Клиентом. Управление аутентификационным приложением переносится из приложения мобильного банка на аутентификационный сервер



# Принципиальная схема аутентификации пользователя мобильного приложения с установкой защищенного соединения

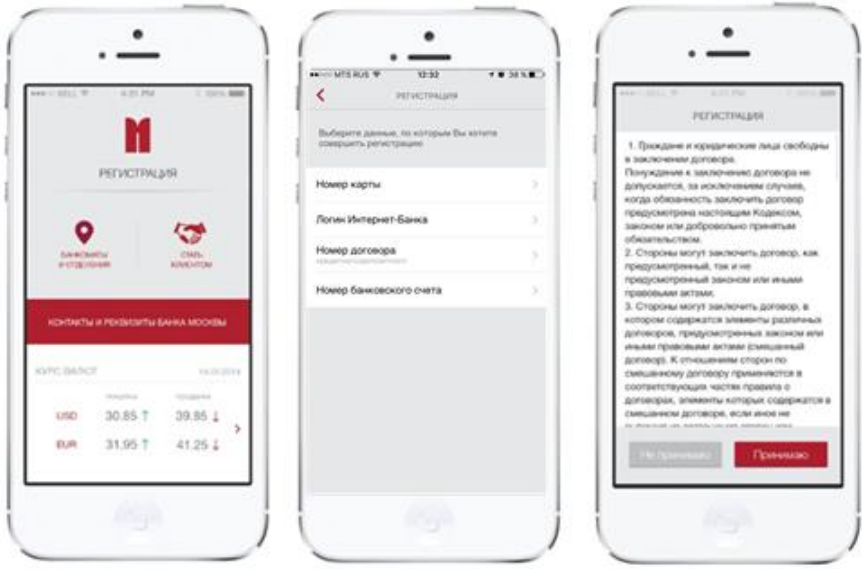


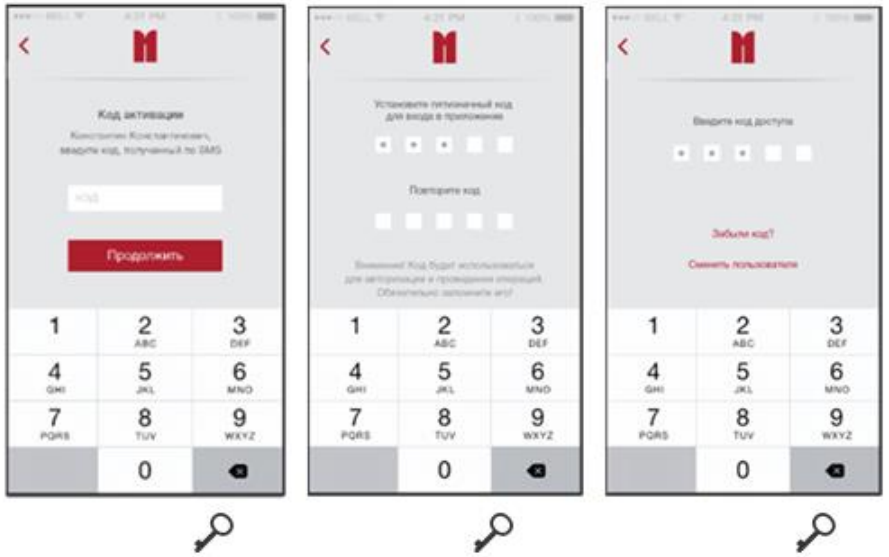
# Принципиальная схема верификации транзакций

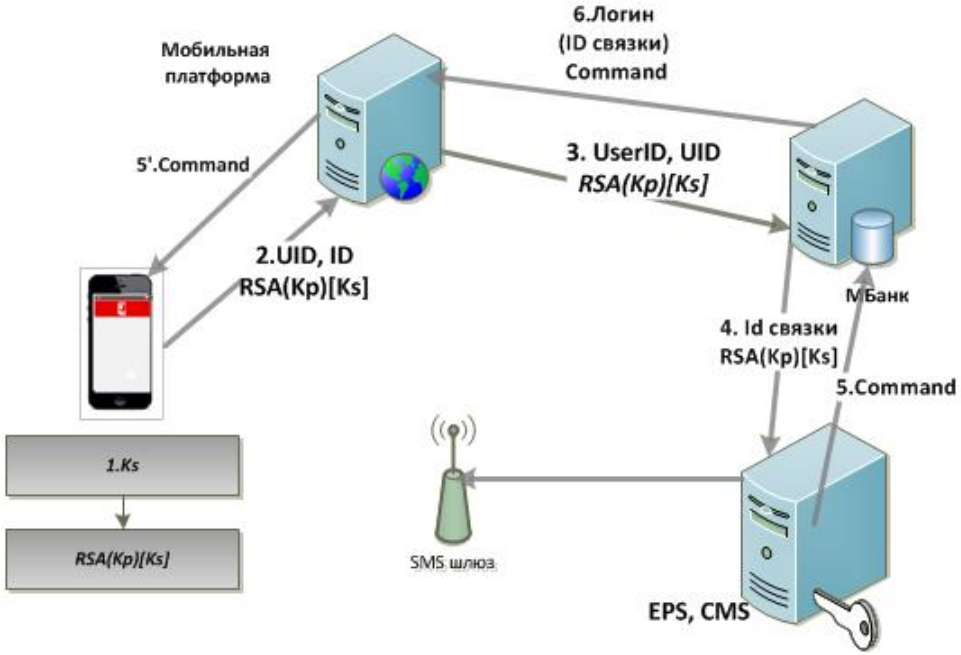


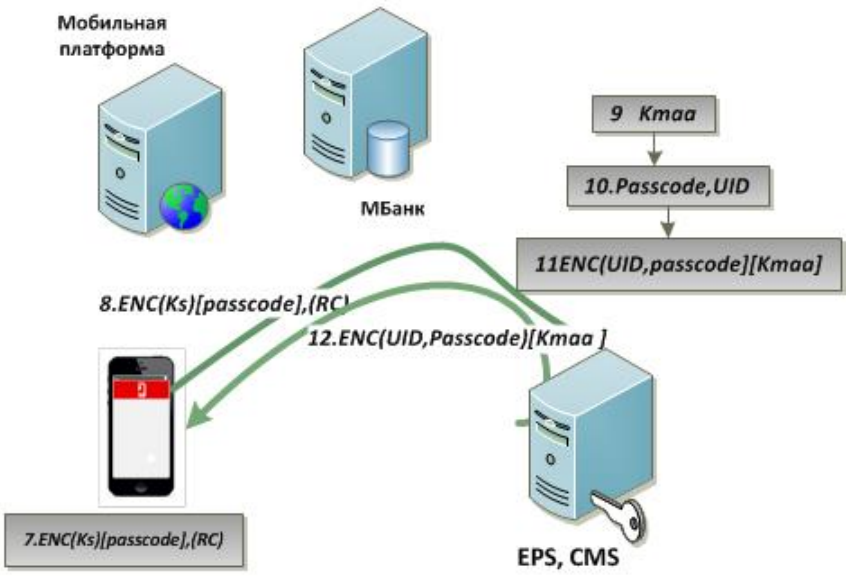
# Регистрация приложения мобильного банка

Банк Москвы



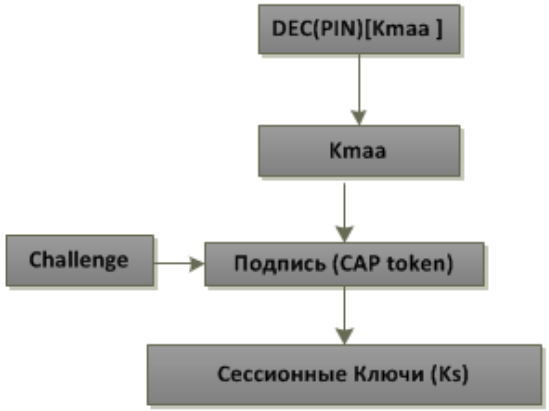


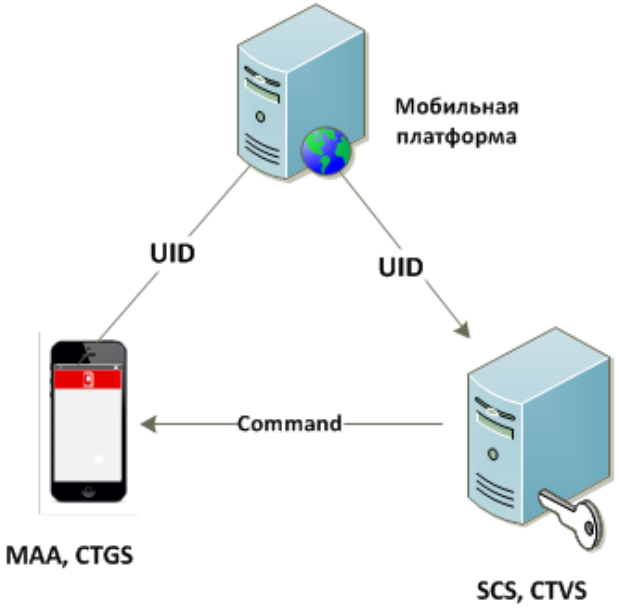


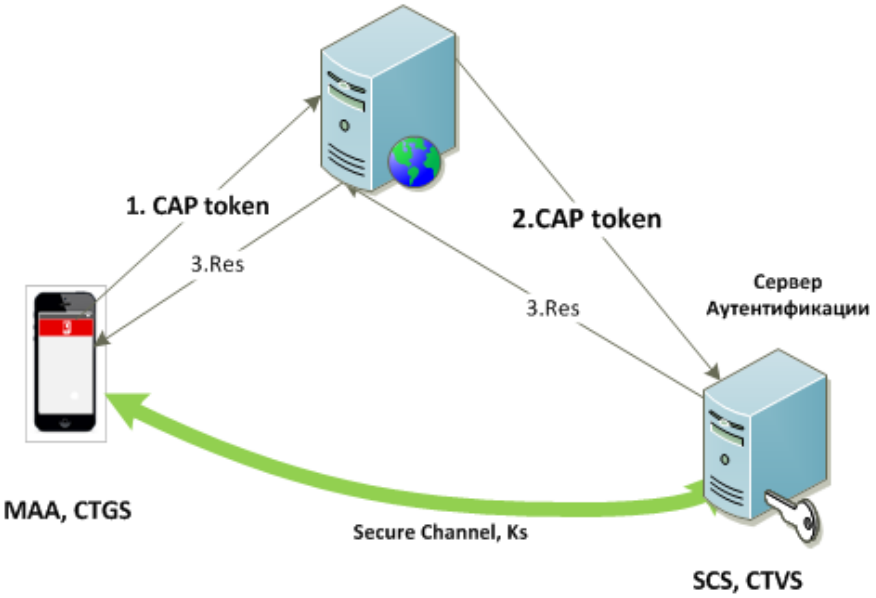



# Аутентификация

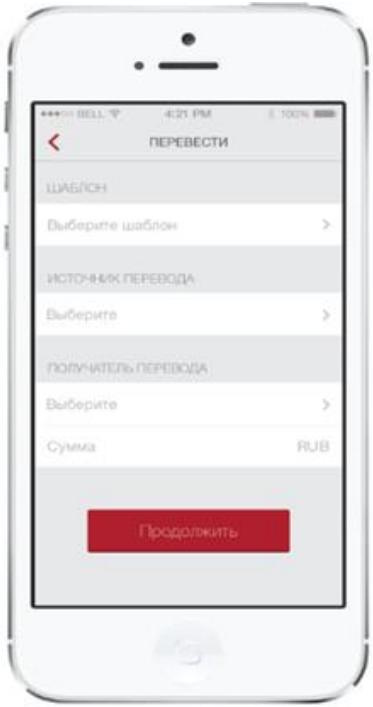
Банк Москвы

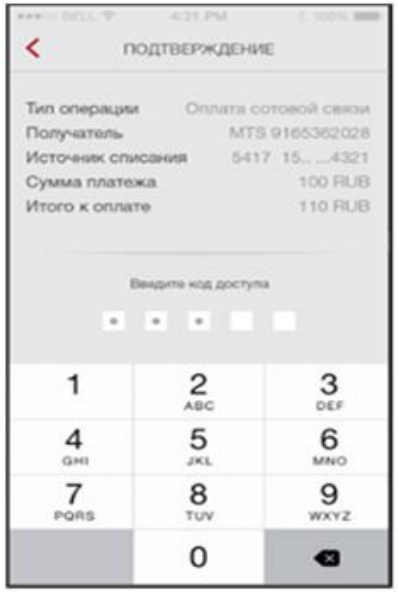



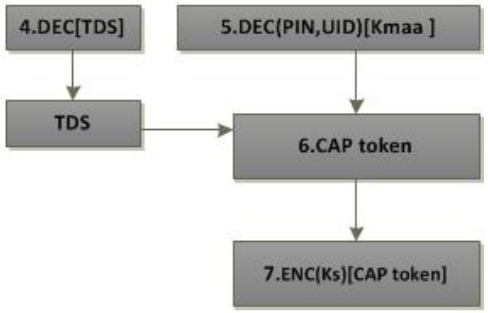



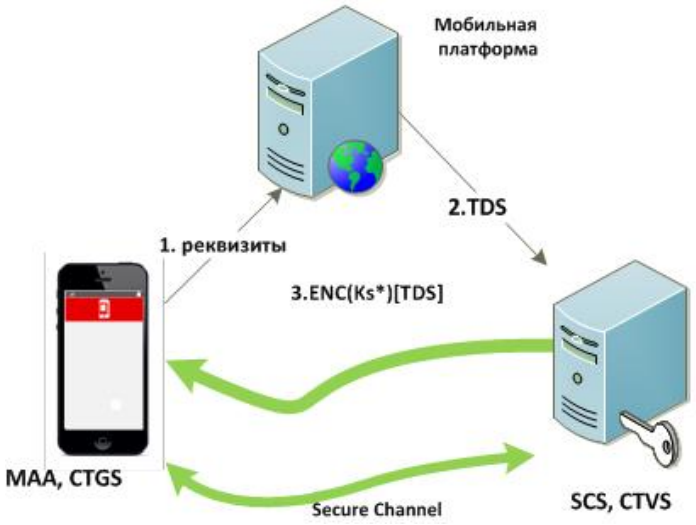



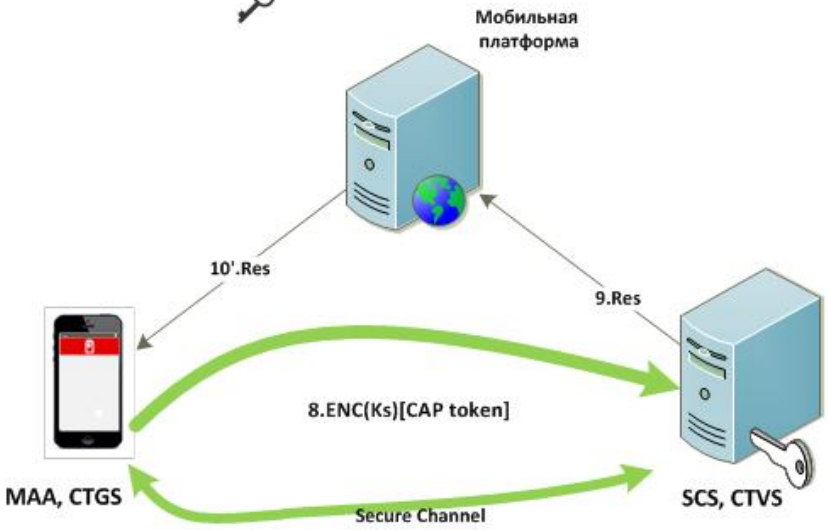
# Верификация



# Требования к SDK

Банк Москвы

| Функциональные требования | Техническое решение |
|---|---|
| •Защищенный канал | • Аутентификационные данные передаются между SDK и сервером аутентификации по защищенному каналу<br>• Между приложением мобильного банка и платформой устанавливается TLS соединение с использованием SSL pinning |
| •Защита от реверс-инжиниринга | Обфускация исполняемого кода |
| •Защита чувствительных данных на мобильном устройстве | •Используется шифрование на значениях Passcode и Device Fingerprint<br>•Используется защищенные клавиатура и экранные формы |
| •Защита пароля клиента | Значение Passcode не хранится на мобильном устройстве и сервере аутентификации |
| •Jailbreak и Root Detection | Отслеживание джейлбрейка (jailbreak) и Root – прав перед вводом Passcode и извлечением ключей мобильного аутентификационного приложения из защищенного хранилища |

# Защита от атак

Банк Москвы

| Функциональные требования | Техническое решение |
|---|---|
| Brute Force | Контроль значений Passcode осуществляется на сервере аутентификации. |
| Man-in-the-middle | Для установки защищенного соединения между maa (SDK) и сервером аутентификации сессионные ключи генерируются параллельно на знании общего секрета без обмена критической информацией. . |
| Phising & Pharming<br>Man-in-the-browser | URL мобильной платформы зашит в исполняемом коде и все аутентификационные данные генерируются на уникальном ключе MAA. |
| Копирование чувствительных данных на другое устройство | Чувствительные данные хранятся в защищенном хранилище. |