

Сведения об эксплуатации экземпляра программы

«Система динамического управления диапазонами SIM-карт Forward DSA»

Правообладатель:
ООО «Форвард-Телеком»

Forward DSA (Dynamic SIM Allocation) – является информационной системой динамического управления диапазонами SIM-карт. DSA дает возможность производить и распространять один общий тип SIM-карт для любого типа мобильных услуг: предоплаченные, постоплатные, SIM-карты для передачи данных. Это позволяет операторам распространять SIM-карты по разным каналам с использованием одного общего типа SIM-карты и предоставлять их в сети только в случае необходимости отказавшись от предварительной подготовки SIM-карт.

С помощью решения DSA операторы мобильной связи могут оптимизировать процесс производства и распространения SIM-карт за счет внедрения эффективной логистики, значительной экономии средств и устранения зависимости от срока действия SIM-карт. Система поддерживает кластерное масштабирование и может использоваться в распределенных сетях крупных федеральных и региональных операторов связи.

Контактная информация: support@fw-t.ru

1 Общая информация

Forward DSA предназначена для гибкого распределения SIM-карт и управления их активацией. Она позволяет оператору мобильной связи оптимизировать использование SIM-карт и упростить их активацию в момент, когда абонент начинает пользоваться услугами.

При производстве SIM-карт используются временные диапазоны IMSI_TEMP (временный технологический/фиктивный идентификатор IMSI), которые позволяют получить универсальную «динамическую» SIM-карту без привязки к региону, способную регистрироваться в сети через специальный HLR_TEMP для последующего взаимодействия с OTA-платформой и получения командных SMS для присвоения целевых региональных идентификаторов IMSI_REG и MSISDN_REG.

Файлы с данными о SIM-картах от производителя загружаются в биллинговую систему Forward для дальнейшей продажи абонентам и провиженинга ключевой информации на элементы сети оператора (HLR/AuC/OTA)

DSA обеспечивает:

1. Загрузку и учёт SIM-карт

Загрузка SIM-карт со временными номерами в систему Forward производится с помощью зашифрованных файлов специального формата. Данные SIM-карты не привязаны к какому-либо региону. При загрузке данных SIM, ключи KI и OTA сохраняются в защищенном хранилище Key Storage.

2. Подключение нового Абонента

При подключении новых Абонентов в любом из каналов продаж используется SIM без региональной привязки. Процесс состоит из 2-х этапов: Резервирование временных идентификаторов и связка SIM и Регистрация SIM в сети и присвоение целевых региональных идентификаторов

3. Активацию SIM-карт «на лету»

SIM-карты остаются "чистыми" (без привязки к определенному номеру) до их первой активации. При вставке SIM-карты в устройство система обновляет профили SIM-карты через кампанию OTA в соответствии с выбранными услугами и номером.

4. Использование вебсервисов

Подсистема DSA предоставляет следующие вебсервисы (REST API):

- a) keystore API - предоставляет методы для работы с Key Storage модулем, а именно:
 - работа с профилями шифрования
 - управление ключами шифрования
 - сохранение и получения защищенной информации
- b) DSA API – реализует внутренние методы необходимые для взаимодействия DSA модуля с Forward Billing и Forward SP системами.

с) XDRay API – для уведомления системы DSA о первой регистрации SIM карты абонента с временными идентификаторами в сети оператора.

5. Оптимизацию затрат

Модуль позволяет минимизировать затраты, связанные с преднастройкой SIM-карт. SIM-карты не нуждаются в предварительном присвоении номера, что снижает риск ошибок или потерь.

6. Гибкость для операторов

Оператор мобильной связи получает возможность динамически управлять пулами номеров, SIM-картами и настройками, подстраиваясь под текущие запросы и нагрузку.

2 Эксплуатация системы

2.1 DSA-процесс

Загрузка SIM-карт со временными номерами в систему Forward производится с помощью зашифрованных файлов специального формата. Данные SIM-карты не привязаны к какому-либо региону. При загрузке данных SIM, ключи KI и OTA сохраняются в защищенном хранилище Key Storage.

При подключении новых Абонентов в любом из каналов продаж используется SIM без региональной привязки. Бизнес-процесс DSA выполняется в автоматическом режиме и состоит из двух этапов:

1. DSA Этап 1, Резервирование временных идентификаторов и связка SIM.

В рамках заказа на подключение нового абонента в системе выбирается регион подключения, мобильный номер и тарифный план/офер.

Для последующего присвоения SIM-карте в биллинговой системе резервируются необходимые постоянные идентификаторы:

- IMSI_REG – целевой IMSI из регионального пула,
- MSISDN_REG – постоянный MSISDN из закреплённого за выбранным регионом (возможен ручной выбор).

Далее в процессе обработки заказа в биллинговую систему передаётся/указывается ICCID подключаемой SIM-карты, который связан с временным значением IMSI_TEMP из пула временных идентификаторов (без региональной привязки) и временным MSISDN_TEMP.

Данная SIM-карта регистрируется в сети оператора на HLR_TEMP с использованием предварительной связки IMSI_TEMP, произведённой при производстве SIM, и MSISDN_TEMP, и на OTA платформе, для возможности последующего присвоения целевых региональных идентификаторов посредством OTA.

Параллельно биллинговая система инициирует связку IMSI_REG + MSISDN_REG, и провиженинг IMSI_REG/MSISDN_REG на региональные сетевые узлы оператора

2. DSA Этап 2, Регистрация SIM в сети и присвоение целевых региональных идентификаторов.

Абонент самостоятельно устанавливает SIM-карту в устройство и регистрируется в сети. По факту первой регистрации SIM в сети, мы получим оповещение из сети посредством вызова специального API, после чего будет инициирована OTA кампания по отправке командной SMS с IMSI_REG через OTA-платформу.

В рамках OTA кампании OTA-платформа отправляет технические SMS для обновления SIM-апплета на SIM-карте. После обновления данных на SIM карте производится пере-инициализация SIM-карты с региональными идентификаторами на терминале. Биллинговая система, после подтверждения о успешном применении

командной OTA-SMS с целевыми значениями IMSI, отправляет команды на удаление временной связки IMSI_TEMP и MSISDN_TEMP с HLR_TEMP.

2.2 Вебсервисы DSA

DSA предоставляет следующие вебсервисы (REST API):

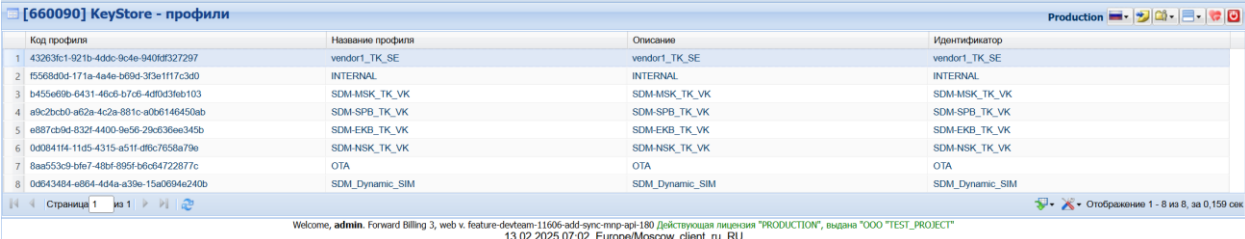
1. keystore API - предоставляет методы для работы с Key Storage модулем, а именно:
 - работа с профилями шифрования
 - управление ключами шифрования
 - сохранение и получения защищенной информации
2. DSA API – реализует внутренние методы необходимые для взаимодействия DSA модуля с Forward Billing и Forward SP системами.
3. SIM Registration API – для уведомления системы DSA о первой регистрации SIM карты абонента с временными идентификаторами в сети оператора.

2.3 Управление настройками и конфигурированием DSA-процесса

2.3.1 Справочники

2.3.1.1 «Профили Шифрования»

Справочник «KeyStore - профили» является поисковым интерфейсом и предназначен для вывода информации о профилях шифрования заведенных в модуле Keystore системы DSA.



Код профиля	Название профиля	Описание	Идентификатор
1 43263c1-921b-4ddc-9c4e-9406f327297	vendor1_TK_SE	INTERNAL	vendor1_TK_SE
2 f56880d-171a-4a4e-b69d-3f3e1117c3d0	INTERNAL	INTERNAL	INTERNAL
3 b455e69b-6431-46c6-b7c6-4d0d31ab103	SDM-MSK_TK_VK	SDM-MSK_TK_VK	SDM-MSK_TK_VK
4 a9c2bcb0-a62a-4c2a-881c-a0b6146450ab	SDM-SPB_TK_VK	SDM-SPB_TK_VK	SDM-SPB_TK_VK
5 e887cbd9-832f-4430-9e56-29c336ee345b	SDM-EKB_TK_VK	SDM-EKB_TK_VK	SDM-EKB_TK_VK
6 d0d84114-11d5-4315-a51f-d86c765ba79e	SDM-NSK_TK_VK	SDM-NSK_TK_VK	SDM-NSK_TK_VK
7 8aa553c9-b6f7-48bf-895f-b6c94722877c	OTA	OTA	OTA
8 d0d43484-e864-4d4a-a39e-15a0094e240b	SDM_Dynamic_SIM	SDM_Dynamic_SIM	SDM_Dynamic_SIM

Выводится следующая информация по каждому профилю шифрования из KeyStore:

- Код Профиля – уникальный идентификатор профиля шифрования в модуле Keystore
- Название профиля
- Описание
- Идентификатор – внешний идентификатор для профиля

2.3.1.2 «KeyStore - ключи»

Справочник «KeyStore - ключи» предназначен для вывода информации о имеющихся ключах шифрования для профилей шифрования заведенных в модуле Keystore системы DSA.

[660091] KeyStore - ключи				Production
Код ключа	Код профиля	Дата С	Дата До	
1 e11964b2-4450-4a6f-9f8b-7c09011aeb99	43263c1-921b-4ddc-9c4e-94069327297	31.12.2019 22:00:00	31.12.2099 22:00:00	
2 3b7c9eef-0eaa-4c59-ad36-b6296363de41	f5568d5d-171a-4a4e-b69d-3f3e1f17c3d9	31.12.2019 22:00:00	31.12.2099 22:00:00	
3 2c18a970-1623-4607-a62e-aaa57814cd05	b455e69b-6431-46c5-b7c6-4d0d3f6b103	31.12.2019 22:00:00	31.12.2099 22:00:00	
4 64a710ae-0d96-430f-935e-1f28b6b2088	a9c2bcd0-a62a-4c2a-881c-a0b6146450ab	01.01.2020 01:00:00	01.01.2100 01:00:00	
5 46ef1764-b05e-4a7d-990c-c67213c11c3c	e887cb9d-832f-4400-9e56-29c636ee345b	01.01.2020 01:00:00	01.01.2100 01:00:00	
6 d0e7e57-0b4e-44be-a0cd-a1d7e8439e27	0d0841f4-11d5-4315-a51f-d86c7658a79e	01.01.2020 01:00:00	01.01.2100 01:00:00	
7 ac2f25fc-cd5c-4f08-9448-bef47531aae2	0d643484-e864-4d4a-a39e-15a0694e240b	01.01.2020 01:00:00	01.01.2100 01:00:00	

Выводится следующая информация по каждому профилю шифрования из KeyStore:

- Код Ключа – уникальный идентификатор ключа шифрования в модуле Keystore
- Код профиля – идентификатор профиля, к которому относится данный ключ
- Дата С – сроки действия ключа
- Дата По – Сроки действия ключа

2.3.1.3 «billing – профили из keystore»

Справочник «billing – профили из keystore» используется для управления взаимосвязями между профилями и вендорами SIM-карт / SDM/AUC в биллинге и соответствующими им профилями шифрования в keystore.

[660092] billing - профили из keystore				Production
Тип профиля: Все выбрано				
Найти Сбросить				
Тип профиля	Наименование профиля	ID профиля в Keystore	Регион	
1 BEELINE	SDM_MSK_TK_VK	b455e69b-6431-46c5-b7c6-4d0d3f6b103	г. Москва, Московская область	
2 VENDOR	vendor1_TK_SE	43263c1-921b-4ddc-9c4e-94069327297		
3 BEELINE	SDM_Санкт-Петербург	a9c2bcd0-a62a-4c2a-881c-a0b6146450ab	г. Санкт-Петербург, Ленинградская область	
4 OTA	OTA	8aa553c9-b7e7-48bf-895f-b6c64722877c		
5 BEELINE_TEMP	SDM_Dynamic_SIM	0d643484-e864-4d4a-a39e-15a0694e240b		

Область поиска в данном справочнике представлена выбором из предлагаемого статического списка типа профиля:

- OTA – означает профиль для системы OTA
- Vendor – профиль для производителя SIM-карт
- HLR_REG – профиль для региональных HLR/AUC («Базовый оператор»)
- HLR_TEMP – профиля для временного HLR/AUC («Временный профиль»)

Таблица результатов поиска представлена списком со следующими колонками:

- «Тип профиля»
- «Наименование профиля» – наименование профиля в биллинге
- «ID профиля в Keystore» – ссылка на соответствующий профиль шифрования в keystore, через его идентификатор.
- «Регион» - MNP регион соответствующий данному профилю

Создание или редактирование связи в системе осуществляется в окне интерфейса:

Скриншот диалогового окна с заголовком "[660092] billing - профили из keystore", Создание записи. В окне три поля ввода: "Тип профиля:" (выпадающий список с значением "ОТА"), "Наименование профиля:" и "ID профиля в Keystore:". Внизу расположены кнопки "Создать" и "Отмена".

- «Тип профиля» – обязательное к заполнению поле наименования типа профиля из списка доступных значений.
- «Наименование профиля» – обязательное наименование профиля.
- «ID профиля в Keystore» – обязательное поле ввода идентификатора профиля шифрования из Keystore.
- «Регион» – обязательное поле только при выборе типа профиля «Базовый оператор», выбирается из списка MNP регион.
- «Вендор» - обязательное поля для типа профиля “VENDOR” – выбирается вендор из списка.

Примечание: для существующих записей доступно редактирование только параметра «ID профиля в Keystore».

2.3.2 Операции Key Storage

Система шифрования чувствительных данных (Key Storage) предоставляет возможности их безопасного хранения и передачи, а именно:

1. Зашифрованное хранение данных в БД системы, с использованием внутреннего ключа шифрования.
2. Шифрование данных при передаче их внешним системам, с помощью транспортных ключей.
3. Дешифрация данных при загрузке, транспортным ключом вендора.
4. Управление профилями и ключами шифрования
5. Ротация ключей шифрования (включая внутренний ключ).
6. Шифрация/Дешифрация Транспортных Ключей при сохранении в базу с помощью Мастер ключа.

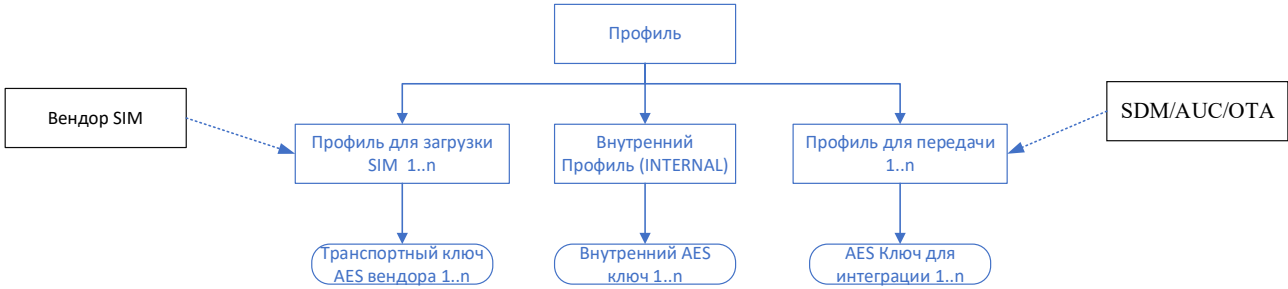
2.3.2.1 Управление профилями и ключами шифрования

Связь между транспортными ключами (ТК) и вендорами SIM или сетевыми элементами осуществляется через «профили» шифрования. Для каждого вендора SIM / SDM / AUC /

ОТА должен быть заведен свой профиль. Затем для каждого профиля добавляются транспортные ключи шифрования стандарта AES 128.

В случае необходимости замены ТК - происходит добавление нового ключа с указанной даты в рамках соответствующего интеграционного профиля. Срок действия старого ключа при этом завершается.

Так же есть системный интеграционный профиль с наименованием «INTERNAL» в рамках которого хранятся внутренние ключи шифрования.



Примечание: Операции с данными в модуле Keystore выполняются только через REST API

2.3.2.2 Профили

Профиль содержит следующие параметры:

Параметр	Тип	Обязательность	Описание
id	UUID	Да, генерируется автоматически системой	Уникальный идентификатор профиля
name	текст	Да	Наименование профиля
description	текст	нет	Описание
extIdent	текст	Да	Системное наименование профиля (для внешних интеграций и поиска). Должен быть уникален.

Система поддерживает следующие операции с профилями:

1. Создание нового профиля (POST /encryption/profile). При создании нового профиля система проверяет уникальность параметра extIdent и не позволяет создать профили с одинаковым значением.
 - а) После создания профиля для вендора SIM, идентификатор профиля необходимо указать в качестве значения параметра «ID профиля в Keystore» в справочнике #Flexy660092 «billing – профили из keystore» для соответствующего вендора. Таким образом система будет определять профиль шифрования и соответствующие транспортные ключи шифрования, при загрузке файла с SIM-картами от производителя.
 - б) После создании профиля для региональных сетевых элементов (HLR/AUC), необходимо их привязать к соответствующему региону в справочнике

#Flexy660092 «billing – профили из keystore» для типа профиля «Базовый оператор» и указать идентификатор профиля в качестве значения параметра «ID профиля в Keystore». Предполагается, что одному региону может соответствовать только один профиль сетевого элемента.

с) Профили для временного коммутатора (HLR_TEMP) и OTA – не привязываются ни к какому региону. Предполагается, что в системе может быть только по одному профилю шифрования для временного AUC и OTA платформы.

2. Редактирование следующих параметров профиля (PATCH /encryption/profile/{profileId}):
name
description
3. Поиск и отображение списка существующих профилей в системе
4. Удаление профиля (DELETE /encryption/profile/{profileId}).
5. Отображение ключей шифрования для профиля (GET /encryption/profile/{profileId}/keys)

2.3.2.3 Ключи шифрования

У ключей шифрования в системе имеются следующие параметры:

Параметр	Тип	Обязательность	Описание
id	UUID	Да, генерируется автоматически системой	Уникальный идентификатор ключа
profileId	UUID	Да	Ссылка на интеграционный профиль, которому принадлежит ключ
startDateTime	Дата	Да	Дата начала действия ключа
endDateTime	Дата	Да	Дата окончания действия ключа
keyValue	Текст	Да	Значение ключа

Система поддерживает следующие операции с ключами:

1. Добавление нового ТК (POST /encryption/key). Ключ заранее должен быть сгенерирован для алгоритма симметричного блочного шифра AES (128), с режимом ECB. И зашифрован публичным мастер ключом. Уже зашифрованное значение указывается при добавлении ключа. Помимо самого значения ключа, пользователь также указывает все остальные обязательные параметры. Далее система проверяет:
 - валидность ключа путем попытки его дешифрации с помощью приватного мастер ключа.
 - отсутствие пересечения с периодом действия других ключей данного профиля. В случае обнаружения пересечения система прервет операцию с соответствующей

ошибкой. Для исправления необходимо удалить или закрыть(путем редактирования периода действия) текущий ключ. ВНИМАНИЕ: Добавление нового ключа для профиля "INTERNAL" требует перешифровку текущих защищенных данных новым ключом. Для чего необходимо запустить специальную процедуру.

2. Удаление ключа (DELETE /encryption/key/{keyId}). Система запрещает удалять ключ для профиля INTERNAL, если им зашифрованы какие-либо данные в хранилище.
3. Редактирование периода действия существующего ключа (PATCH /encryption/key/{keyId})
4. Просмотр списка созданных ключей.

2.3.2.4 Добавление данных (SIM-карт) в keystore

1. При загрузке файла с SIM-картами от производителя система, на основании формата файла, определяет наличие защищенных данных/полей и в случае наличия таких, выполняет дальнейшие шаги. Формат файла для каждого вендора будет согласован и реализован в рамках процесса внедрения.
2. Для указанного при загрузке вендора, определяет связанный профиль шифрования в keystore, согласно конфигурации справочника #Flexy660092 «billing – профили из keystore». Если актуального профиля не найдено – то операция прерывается и возвращается ошибка.
3. Для каждого значения параметра из файла, который надо сохранить в защищенном хранилище keystore вызывается операция:
 - a) разового добавления: POST /encryption/store
 - b) либо массового добавления значений POST/encryption/store/raw
 - c) в рамках которой передаются следующие данные:
 - d) masterType - тип сущности, к которой принадлежит сохраняемый параметр, например ICCID
 - e) masterInst – идентификатор сущности
 - f) valueType – наименование параметра у сущности, значение которого нужно сохранить в keystore, например EK1, KIC1, KID1, KIK1 и т.д.
 - g) encryptedValue – значение параметра, зашифрованное транспортным ключом вендора
 - h) profileId – идентификатор профиля вендора в keystore
 - i) dateTime – опционально, дата на которую надо брать ТК вендора. Если не указана – используется текущая дата.
4. В рамках выполнения операции, система для указанного профиля получает актуальный на текущий момент времени транспортный ключ. Если актуального ТК не найдено – то операция прерывается и возвращается ошибка.

5. Т.к. транспортные ключи хранятся тоже зашифрованными, то полученный транспортный ключ расшифровывается с помощью приватного мастер ключа.
6. С помощью ТК производится расшифровка защищенных данных согласно алгоритму симметричного блочного шифра AES (128), с режимом ECB. В случае невозможности расшифровать параметры данным ключом операция загрузки прерывается
7. Расшифрованные данные шифруются актуальным Внутренним Ключом шифрования используя тот же самый алгоритм.
8. Зашифрованные значения сохраняются в базу данных KeyStorage. При этом для каждого сохраненного значения указывается идентификатор внутреннего ключа, которым оно было зашифровано.

2.3.2.5 Получение защищенных данных из keystore

В процессах провиженинга информации о SIM-картах на внешние сетевые элементы (AUC/OTA), может потребоваться передать в том числе и защищенные параметры, причем данные передаются в зашифрованном виде – но уже с использованием ТК (транспортного ключа) получателя.

В этом случае система:

1. Для сетевого элемента и его региона определяет связанный профиль шифрования в keystore, согласно конфигурации справочника #Flexy660092 «billing – профили из keystore». Для того что бы в дальнейшем зашифровать передаваемое значение ТК из данного профиля.
2. Далее вызывается операция получения данных из keystore (API GET /encryption/store) в которой передаются следующие параметры:
 - a) masterType - тип сущности, к которой принадлежит сохраняемый параметр, например ICCID
 - b) masterInst – идентификатор сущности
 - c) valueType – наименование параметра у сущности, значение которого нужно получить из keystore, например EK1, KIC1, KID1, KIK1 и т.д.
 - d) profileId – идентификатор профиля получателя значения в keystore
3. В рамках выполнения операции на основании переданного профиля шифрования получает актуальный на текущий момент времени транспортный ключ. Если актуального ТК не найдено – то операция прерывается и возвращается ошибка.
4. Полученный транспортный ключ расшифровывается с помощью приватного мастер ключа.
5. Необходимое значение защищенного параметра считывается из БД KeyStorage, и расшифровывается с помощью внутреннего ключа, которым оно было зашифровано, согласно алгоритму симметричного блочного шифра AES (128), с режимом ECB.
6. Расшифрованное значение параметра зашифровывается Транспортным Ключом сетевого элемента и передается во вне.

2.3.2.6 Дополнительные операции Keystore

Помимо вышеперечисленных операций, keystore поддерживает следующие дополнительные операции:

1. GET /encryption/store/raw - Получение из хранилища значения в открытом виде
2. DELETE /encryption/store/{masterType}/{masterInst}/{valueType} Удаление значения из хранилища

2.3.2.7 Ротация Ключей

В системе существуют следующие логические виды ключей:

1. Мастер Ключ (RSA) – с помощью которого шифруются и дешифруются транспортные и внутренние ключи.
2. Транспортный Ключ (ТК - AES) – ключ, который используется для шифрования/дешифрования данных при интеграции с внешними системами или загрузки информации.
3. Внутренний ключ (AES) – используется для шифрования защищенных данных при сохранении в БД системы Key Storage.

Все виды ключей должны обновляться при подозрении на компрометацию или при достижении максимального срока использования. Но для разного вида ключей этот процесс происходит по-разному.

1. Замену мастер ключей производит только техническая поддержка FW по запросу. В процессе его замены происходит перешифрация всех транспортных ключей и внутреннего ключа. На этот короткий период система недоступна для использования.
В случае подозрения на компрометацию мастер ключа рекомендуется так же произвести замену всех транспортных ключей и внутреннего ключа.
2. Замена транспортных ключей может производиться в любое время, путем удаления (закрытия) старого ключа и добавления нового. После такой замены – все последующие операции шифрования/дешифрования при интеграциях и загрузки файлов будут производиться с новым ключом. Поэтому данная операция должна быть синхронизирована с вендорами/внешними партнерами.
3. Замена внутреннего ключа происходит таким же способом, как и остальных транспортных ключей, только указывается интеграционный профиль INTERNAL. НО после этого вручную инициируется процедура перешифрации хранимых данных новым ключом. Данная процедура выполняется асинхронно и останавливает предоставление сервиса на период выполнения. Алгоритм:
 - a) В качестве входного параметра процедуры передается новый внутренний ключ шифрования.
 - b) После чего процедура производит поиск всех элементов в хранилище, зашифрованных отличными ключами от переданного.

- с) Далее система поочередно производит дешифрацию элемента старым ключом и шифрацию новым

После обработки всех элементов из списка, процедура перешифровки считается завершенной.

2.3.3 Загрузка SIM

Информация о SIM-картах передается от производителя (вендора) в виде текстового файла, определенного формата.

Вендоров может быть несколько, список будет согласован в рамках процесса внедрения.

Для каждого вендора будет согласован определенный формат файла и имплементирован в рамках процесса внедрения.

В файле должна содержаться, как минимум, следующая обязательная информация для SIM-карт:

- ICCID
- IMSI
- EKi
- OTA-ключи

Значения ключей аутентификации SIM EKi в файле зашифрованы с помощью транспортного ключа вендора.

2.3.3.1 Конфигурация Вендора

1. Согласованный список вендоров будет заведен в справочнике при настройке.
2. Для каждого вендора добавляется один профайл шифрования (необходим для хранения транспортных ключей шифрования вендора).
3. Транспортный Ключ вендора добавляется в профиль.

2.3.3.2 Загрузка информации о SIM в систему

Интерфейс массовой обработки «Загрузка SIM-карт» предназначен для загрузки из файла списка SIM-карт с последующей настройкой обработки информации и запуска процесса создания экземпляров. В качестве параметров для массовой обработки необходимо указать:

- Тип SIM карты;
- Департамент
- Дата, на которую надо брать транспортный ключ для расшифровки файла
- Вендор - Так как производителей SIM может быть несколько, то в рамках процедуры загрузки указывается вендор из списка от которого получен файл.
- Файл с данными о SIM картах.

Примечание: параметры SIM: EKi, должны быть зашифрованы с помощью ТК вендора в файле симметричным транспортным ключом вендора (AES 128b), который согласован заранее и сохранен в соответствующем интеграционном профиле вендора.

По нажатию кнопки «Запуск» происходит массовая загрузка SIM карт в систему из файла. В результате выполнения массовой операции:

1. Информация о SIM-картах и их параметрах загружается в систему, формируются экземпляры SIM-карт. Статус загруженных SIM-карт проставляется «new».
2. Значения ключей аутентификации (EKi и OTA) SIM-карты сохраняются в специальное Key Storage хранилище в зашифрованном виде, с помощью внутреннего ключа хранения.
3. В случае если в загрузочном файле с SIM-картами предоставлены значения IMSI, система автоматически производит связку создаваемых экземпляров SIM-карт с данными IMSI (попутно создавая экземпляры IMSI в системе, при необходимости).