Загрузчик ключей шифрования для радиостанций стандарта TETRA

Руководство пользователя

Версия 1.1

(c) Интегра Про 2026

Содержание

Свидетельство о регистрации 3

Документы 4

Сокращения и термины 5

Введение 6

- Ключи аутентификации TETRA 6

- Статические ключи шифрования 6

- Создание, подготовка и доставка ключей 6

Управление ключами 8

- Общие сведения 8

- Группирование ключей 9

Ключи шифрования в радиостанциях 9

- Условия для реализации шифрования 9

- SCK Grouping Type, SCK Subsets и KAG 10

- Расчет и загрузка ключей SSCK в радиостанцию 11

Работа с программой 12

- Подключение радиостанции 12

- Редактирование и запись ключа K 14

- Редактирование и запись номера SCK Subset 16

- Редактирование ключей SCK и запись SSCK 16

- Результаты выполнения программы 17

Безопасность 20

Свидетельство о регистрации

На программное обеспечение "Загрузчик ключей шифрования для радиостанций стандарта TETRA" получено Свидетельство о государственной регистрации программы для ЭВМ №2026664970 от 19.05.2026г.



РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2026664970

«Загрузчик ключей шифрования для радиостанций стандарта TETRA»

Правообладатель: *Общество с ограниченной ответственностью "Интегра Про" (RU)*

Заявка № 2026663715

Дата поступления 29 апреля 2026 г.

Дата государственной регистрации в Реестре программ для ЭВМ *19 мая 2026 г.*

Руководитель Федеральной службы по интеллектуальной собственности

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат 00a5709d77ad3d1531b4b88188e75f29506

Владелец: Зубов Юрий Сергеевич

Действителен с 04.03.2025 по 28.11.2026

Ю.С. Зубов

Документы

Номер	Название
MOD-11-1279	SKMS Installation Guide
SFPG Rec01	TETRA MoU Security and Fraud Prevention Group, TETRA Key Distribution, Recommendation 01, edition 4.
ts_10039606v020101p	ETSI TS 100 396-6 V2.1.1 (2022-10) DMO Security

Сокращения и термины

Термин	Описание
AuC	Authentication Centre - Центр аутентификации системы TETRA
DMO	Direct Mode Operation - работа на прямом канале TETRA
K	Authentication Key - ключ аутентификации
SCK	Static Cipher Key - статический ключ шифрования
SCKN	SCK Number - номер статического ключа шифрования
SCK-VN	SCK Version Number - номер версии статического ключа шифрования
SFPG	TETRA Association Security and Fraud Prevention Group
SKMS	Standalone Key Management System
SSCK	Sealed SCK - зашифрованный набор ключей SCK
SwMI	Switching and Management Infrastructure - система связи TETRA
TEI	Terminal Equipment Identity - уникальный идентификатор абонента TETRA
TMO	Trunked Mode Operation - системный режим работы абонента TETRA

Введение

Ключи аутентификации TETRA

Система безопасности TETRA базируется на "секретном ключе аутентификации K", известном только радиостанции и AuC (Центру аутентификации системы TETRA). Аутентификация является результатом работы механизма запрос/ответ, не использующего непосредственно сам ключ K для предотвращения его раскрытия; и правильный ответ на запрос возможен только при знании ключа K. Как правило, исходный ключ K используется в течение всего времени жизни радиостанции, хотя ключ может быть переназначен при ее ремонте или по требованиям политики безопасности потребителя. Применение аутентификации в системе TETRA является опциональным.

Для сохранения значения ключа K в секрете его транспортировка от места генерации до радиостанции и до AuC должна выполняться защищенным образом. Кроме того, Центр аутентификации должен иметь возможность сопоставить ключ аутентификации с идентификатором абонента (ITSI), присвоенным терминалу обычно в более позднее время.

Статические ключи шифрования

Статические ключи (SCK) необходимы для шифрования радиоканала в режиме TMO в системах TETRA, применяющих шифрование Security Class 2 как при нормальной работе, так и в аварийном режиме (Fallback mode), а также для работы радиостанций с шифрованием в режиме DMO. В случае DMO ключ SCK выполняет роль аутентификации радиостанции. Радиостанции TETRA могут хранить до 32 ключей SCK, часть из них используется для работы в режиме TMO, часть - в режиме DMO. Время жизни ключей SCK определяется политикой безопасности потребителя, числом использующих шифрование радиостанций и объемом шифрованного трафика. Обычной практикой является периодическая замена ключей SCK.

Ключи SCK можно заранее записать в радиостанцию или, где применимо, они могут быть загружены в режиме TMO по радиоканалу. Как правило, SCK загружаются в радиостанцию в зашифрованном виде (sealed), а базой для шифрования является ее собственный ключ аутентификации K. Это означает, что терминалы, использующие SCK, должны заранее иметь ключ аутентификации K, хотя, как указано выше, сама аутентификация опциональна.

Создание, подготовка и доставка ключей

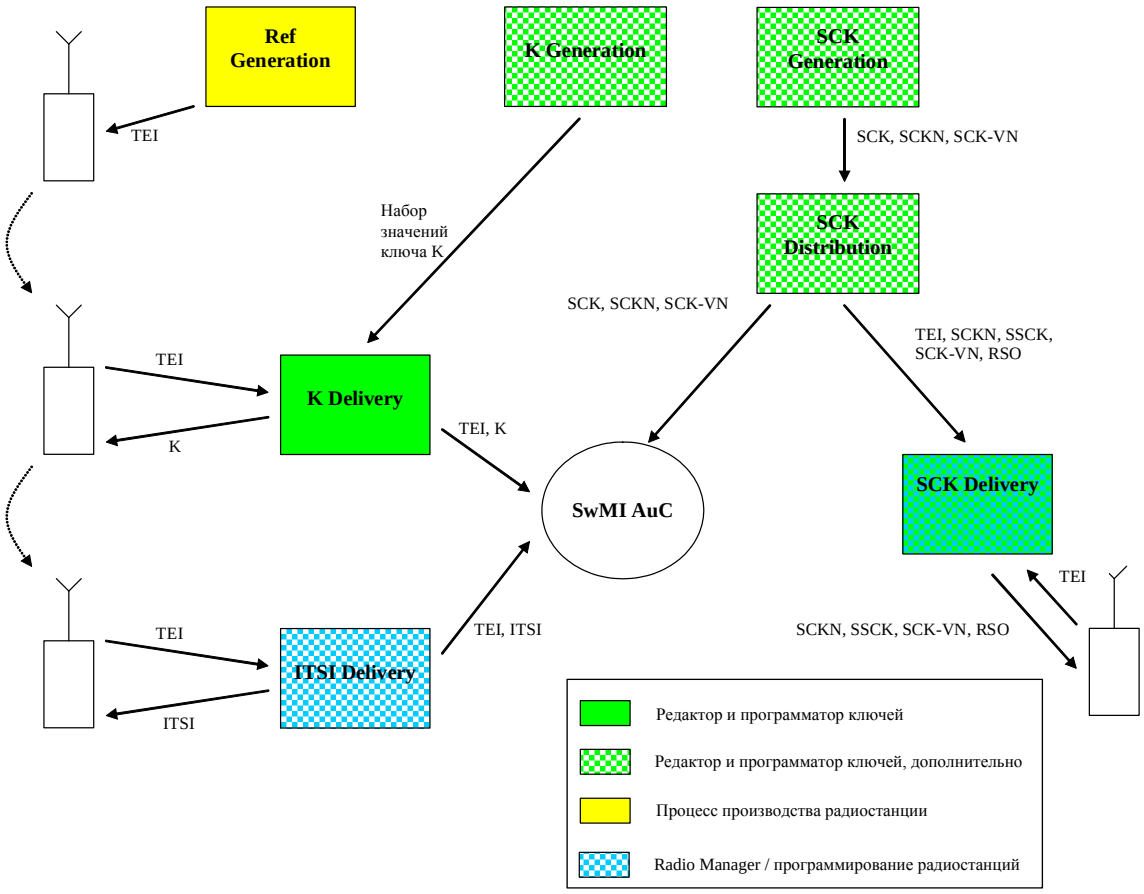
Механизм работы с ключами аутентификации и шифрования описывается стандартом в документе SFPG Recommendation 01 [SFPG Rec01]. Для ключа K предусмотрены следующие элементы:

- Ref Generation - генератор идентификатора оборудования, TEI
- K Generation - генератор ключа K
- K Delivery - доставка ключа K
- ITSI Generation / Delivery - генератор абонентского номера ITSI и его доставка
- SwMI (Authentication Centre) - Центр аутентификации системы TETRA

В работе с ключами шифрования SCK участвуют:

- SCK Generation - генератор ключей SCK
- SCK Distribution - подготовка ключей SCK к доставке
- SCK Delivery - доставка ключей SCK
- SwMI (Authentication Centre - Центр аутентификации системы TETRA).

Ниже приведена общая схема создания и доставки ключей аутентификации и шифрования. Показаны только пути передачи информации, исключая ответы и подтверждения.



Общая схема генерации и распределения ключей

Зеленым цветом выделены задачи, выполняемые Редактором и программатором ключей.

'Ref Generation'означает создание и запись в каждую радиостанцию ее идентификатора TETRA Equipment Identity (TEI) .

'K Generation' с высокой надежностью генерирует 128-битные случайные числа, назначаемые каждой радиостанции в качестве ключа K. Эти данные поступают в 'K Delivery', как правило, в виде файла в формате [SFPG Rec01]. 'K Delivery' импортирует ключи K из файла или может генерировать их самостоятельно.

'K Delivery' отвечает за доставку (запись) ключей K в радиостанции. 'K Delivery' также создает пары 'Ref-K' для отправки в SwMI AuC в виде файла в формате [SFPG Rec01]. В качестве Ref используется TEI радиостанции.

'ITSI Delivery' записывает абонентский номер ITSI (и, возможно, другие данные конфигурации) непосредственно в радиостанцию. Значения ITSI необходимо сообщить SwMI AuC наряду с TEI для идентификации радиостанции. Это позволяет AuC связать значение ключа K радиостанции с ее ITSI.

'SCK Generation' также является высоконадежным генератором 80-битных случайных чисел. В радиостанцию можно записать 32 SCK. Каждому из ключей SCK присвоен номер - SCKN.

Ключ также имеет версию - SCK Version Number (SCK-VN). Набор значений SCK поступает в 'SCK Distribution', как правило, в виде файла формата [SFPG Rec01]. 'SCK Distribution' может их импортировать или создавать самостоятельно .

'SCK Distribution' отвечает за доставку SCK в SwMI и их запись в радиостанции. Обе операции логически разделены, поскольку запись SCK в радиостанции выполняется в полевых условиях.

В случае 'SCK distribution' не отвечает за доставку ключей SCK в SwMI, но необходим для записи SCK в радиостанции, потому что радиостанции Sepura могут загружать SCK только в защищенном (sealed) виде. В радиостанцию загружаются как защищенные ключи Sealed SCKs (SSCK), так и соответствующие им случайные числа Random Seed for OTAR (RSO). Редактор и программатор ключей выполняет запись Sealed SCK в радиостанцию сразу после записи ключа аутентификации К ('K Delivery'), одновременно создавая файл экспорта Sealed SCK для возможного отдельного программатора.

Управление ключами

Приведенные далее сведения заимствованы из документа “ts_10039606v020101p ETSI TS 100 396-6 V2.1.1 (2022-10) DMO Security.pdf”, входящего в пакет документации стандарта TETRA.

Общие сведения

В режиме DMO определен только один тип ключа шифрования - статический ключ шифрования SCK.

SCK выбираются системным администратором и могут быть загружены в радиостанцию в режиме TMO из инфраструктуры (SwMI) с использованием механизма загрузки ключей OTAR, описанного в ETSI EN300 392-7, или запрограммированы вручную.

Выбор и срок службы ключей SCK выходят за рамки настоящего документа и определяются политикой сетевой безопасности организации.

Ключи SCK должны передаваться конфиденциально.

ĭDZÈǽ SCK DzǴQdzǴ ǵHUQǷŊǨǰŽÂ ǰĞǰ QǨǴŽǽdzàž ǨqǰŊǴHU Žǭ 80 ǧŽŊ, ǴǧǴǭdzǨǽǨQDzàǻ ǴŊ SCK(0) QǴ SCK(79). Ключ QǴDZQqdz ǧàŊÂ ǽǨǷŊÂÈ dzǨǧǴHUǨ SCK, ǷǴQqHUQǨøqǨǴ QǴ 32 ǰDZÈǽqž, ǨQǫ ǰǨQQàž ǰDZÈǽ ŽQqdzŊŽÅŽÆŽHUnqŊǷè ǵǴ qǨǴ ǵǴǭŽÆŽŽ Ǩ dzǨǧǴHUǫ (dzǴDzqHU SCKN).

Члены набора SCK могут использоваться различными сетями DMO и могут применяться как в домашней сети радиостанции (Home MNI), так и во внешних сетях.

Для использования в режиме DMO ключи SCK организуются в набор из 30 ключей. При обозначения конкретных элементов этого набора, обозначенных от SCKN(0) до SCKN(29) , используется параметр SCKN, где 1 ≤ N ≤ 30.

SCKN-31 и SCKN-32 (обозначенные как SCKN(30) и SCKN(31)) зарезервированы для использования в транкинговом режиме TETRA и не применяются для шифрования в DMO .

Группирование ключей

Для каждого группового вызова DMO, при котором должно применяться шифрование, у радиостанции должен быть механизм для сопоставления одного или нескольких SCK, идентифицированных SCKN, с идентификатором вызываемой группы (GTSI). В программаторе для этого используются KAG - Key Association Groups.

У SCK должен быть определенный срок службы или срок шифрования. По истечении срока шифрования ключ следует заменить, и радиостанция выбирает другой SCK для передачи. Однако, поскольку DMO является неконтролируемой средой, различные радиостанции могут изменять свой выбор SCK в разное время. Чтобы исключить вероятность сбоя связи SCK сгруппированы в одно или несколько подмножеств для упорядочения процесса управления ключами.

Ключи в разных подмножествах, связанные с одним и тем же групповым идентификатором GTSI, обозначаются термином Key Association Group (KAG). Радиостанция рассматривает один из ключей в качестве текущего и использует этот SCK в качестве ключа для передачи. Любой SCK из KAG может использоваться для приема. Все SCK в KAG должны быть взяты из одного и того же набора SCK и, следовательно, должны быть связаны с одним и тем же MNI. Все ключи в KAG должны быть связаны только с одним алгоритмом TEA.

Там, где используются группы KAG для SCK, в радиостанциях должна быть загружена вся группа KAG , содержащая все ключи SCK .

Ключи шифрования в радиостанциях

Стандартом TETRA предусмотрена работа в режиме DMO с шифрованием с использованием алгоритмов TEA1-TEA7.

Условия для реализации шифрования

Применительно к радиостанциям Sepura, рассмотрим условия, необходимые для реализации работы с шифрованием в DMO.

Радиостанции Sepura второго поколения (GEN2), включающие модели STP8000, STP9000, SRG3900 и ряд других, должны с завода содержать в себе аппаратный модуль шифрования.

Отличить такие радиостанции можно по модельному номеру, например, для модели STP8000 в ее HW-коде на 6-й позиции указывается тип алгоритма шифрования:



В радиостанциях TETRA третьего поколения (GEN3) и ряд других, для работы с шифрованием должна присутствовать соответствующая алгоритму шифрования лицензия:



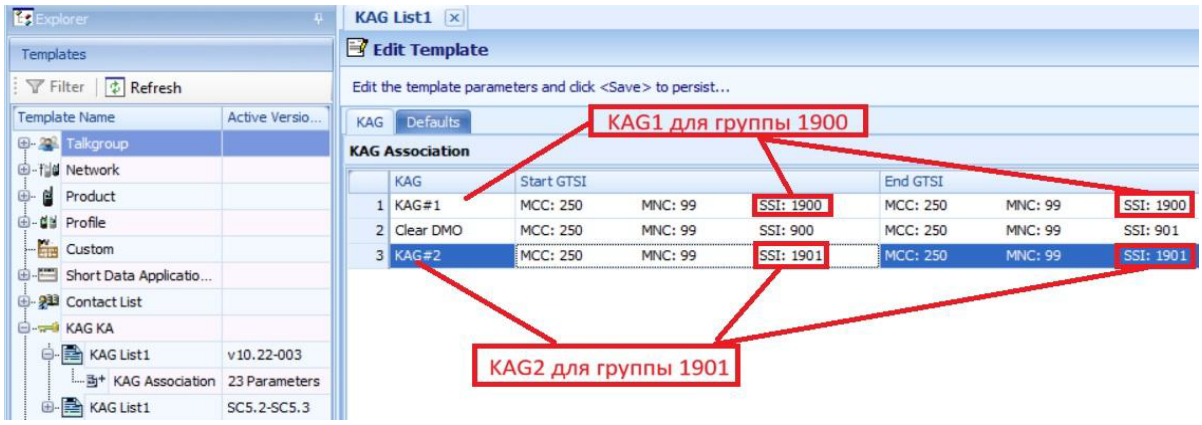
SCK Grouping Type, SCK Subsets и KAG

В каждую радиостанцию загружается набор, содержащий 32 статических ключа шифрования SCK (Static Cypher Key) длиной 80-бит, этот набор является, как правило, общим для всего парка радиостанций организации. По стандарту TETRA ключи с номерами 31 и 32 могут применяться только при работе в режиме TMO.

Набор из 30 ключей DMO может быть организован в подгруппы (SCK Subsets) различным образом, этот параметр называется типом группирования ключей (SCK Grouping Type).

В радиостанциях TETRA применяется исключительно SCK Grouping Type 2, т.е., 3 подгруппы (SCK Subsets) по 10 ключей SCK в каждой. Таким образом, к первой подгруппе относятся SCK1...10, ко второй – SCK11...20, к третьей - SCK21...30.

С другой стороны, в каждой из 3-х подгрупп (SCK Subset), имеющих по 10 ключей SCK, на одинаковой номерной позиции находятся ключи, принадлежащие к одному из 10 наборов KAG (Key Association Groups). Каждой группе DMO, точнее, диапазону номеров групп GTSI назначается определенный номер KAG - от KAG1 до KAG10:



В приведенном выше примере разговорной группе DMO TG1900 назначен KAG1 с тремя входящими в нее ключами: SCK1, SCK11 и SCK21, а TG1901 – KAG2 с тремя входящими в нее ключами: SCK2, SCK12 и SCK22. Диапазону разговорных групп TG900-TG901 не назначены ключи шифрования и эти группы работают в открытом режиме - Clear DMO.

Таким образом, в радиостанциях TETRA каждой разговорной группе DMO, использующей шифрование, назначены сразу 3 ключа шифрования, образующие KAG. Весь диапазон из 30 ключей SCK, в свою очередь, разделен на 3 подгруппы по 10 ключей в каждой: SCK Subset 1=SCK1…SCK10, SCK Subset 2=SCK11…SCK20, SCK Subset 3= SCK21…SCK30.

Только один из трех SCK Subset является активным (Current), и именно его ключ SCK, входящий в KAG для группы, будет использоваться при работе радиостанции в данной разговорной группе на передачу.

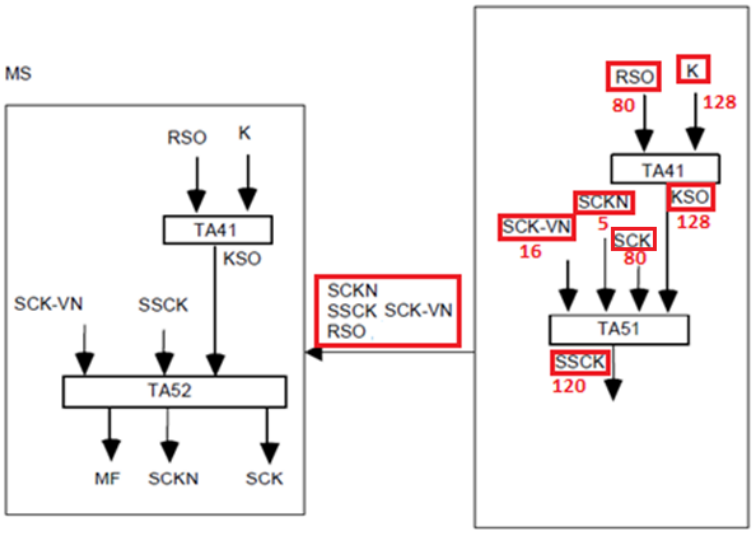
Находясь в группе DMO, радиостанция сканирует на приеме все 3 ключа SCK, входящих в KAG этой группы и, если хотя бы один из этих 3-х ключей совпадает с ключом ведущей передачу радиостанции, она будет принимать разговор группы, несмотря на то, что совпавший ключ может не принадлежать к ее Current SCK Subset, с ключом из которого эта радиостанция работает на передачу.

Ключам SCK может быть определен срок годности, после истечения которого они не должны работать в радиостанции, что потребует периодического обновления набора ключей SCK. Изменив Current SCK Subset ID, можно продолжить работу в группе без потери связи и не спеша заменить утратившие силу ключи в старом наборе SCK Subset.

Расчет и загрузка ключей SSCK в радиостанцию

По соображениям безопасности в радиостанции TETRA невозможно загрузить набор ключей SCK напрямую, вместо этого выполняется загрузка зашифрованного ключевого материала – SSCK (Sealed Static Cypher Keys).

Преобразование SCK->SSCK выполняется по специальному алгоритму, предусмотренному стандартом TETRA:



В создании каждого из 32 ключей SSCK из SCK участвуют следующие величины:

K	- уникальный для радиостанции мастер-ключ, 128 бит, связан с TEI
SCK	- исходный статический ключ шифрования, 80 бит
SCKN	- номер ключа SCK, 5 бит
SCK-VN	- номер версии ключа SCK, 16 бит
RSO	- случайное число, Random Seed, 80 бит

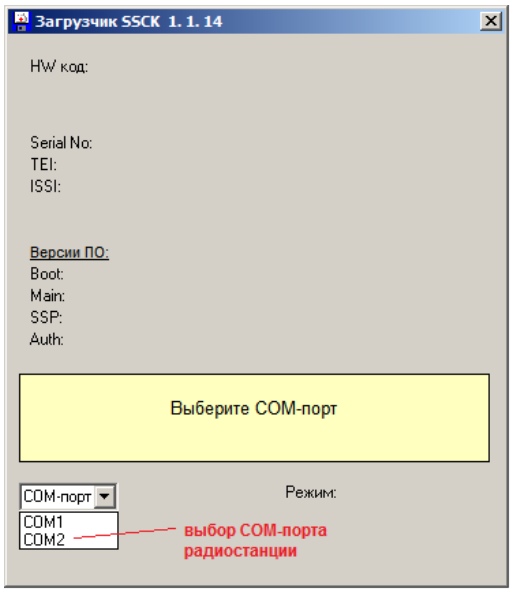
С точки зрения информационной безопасности важно сохранять в секрете значения K и 32-х исходных ключей SCK, и тогда, несмотря на публикацию алгоритма расчета и декодирования ключей SSCK, набор ключей SSCK можно пересылать по открытым каналам.

Расчет и загрузка ключей K и SSCK в радиостанции TETRA выполняется программой 'Загрузчик ключей шифрования для радиостанций стандарта TETRA'.
В ней можно генерировать ключи K и SCK, импортировать и экспортировать данные в формате обмена ключевой информации [SFPG01], предусмотренном стандартом TETRA.

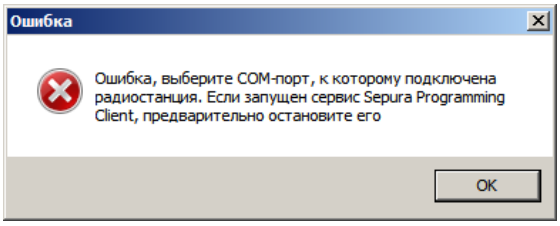
Работа с программой

Подключение радиостанции

Подключите радиостанцию TETRA к COM-порту компьютера соотвествующим кабелем и запустите программу:

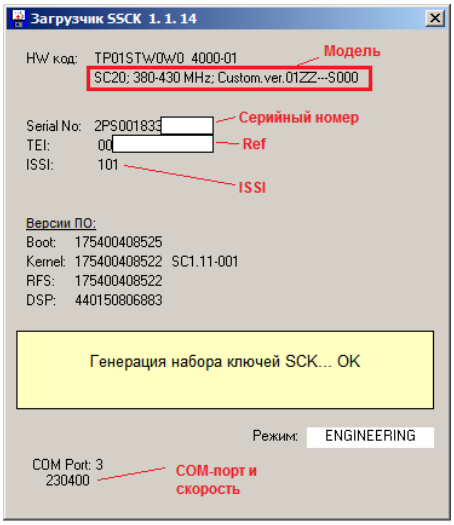


Укажите COM-порт. Если программа не обнаружила радиостанцию, выводится ошибка подключения:

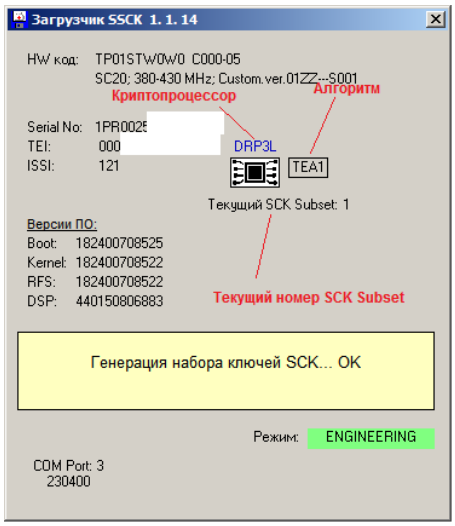


Проверьте правильность выбора COM-порта, включена ли радиостанция и остановлен ли в системе сервис Programing Client (если он присутствует).

При удачном подключении программа выводит данные радиостанции. Если поддерживается работа с шифрованием радиоинтерфейса, показываются модель чипа криптопроцессора, используемый алгоритм шифрования TEA1...TEA4 и текущий номер SCK Subset:

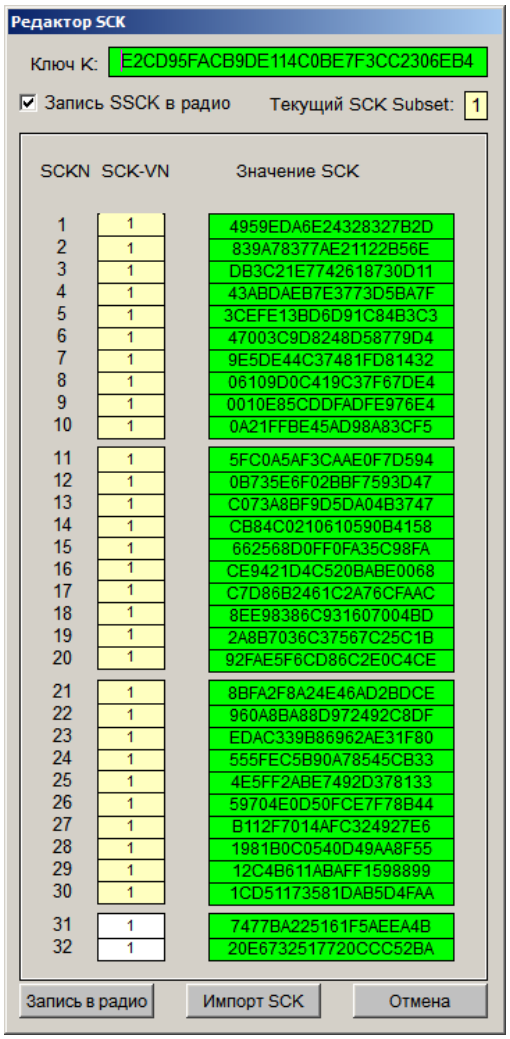


Радиостанция без шифрования



Радиостанция с шифрованием

Одновременно открывется отдельное окно редактора ключей аутентификации K и шифрования SCK:



В окне Редактора в поле 'Ключ К' изначально выводится значение К, предлагаемое программой, которое можно изменять по своему усмотрению.
Следует учесть, что генератор случайного числа К не является высоконадежным, поэтому в ответственных случаях рекомендуется его заменить значением К, полученным из доверенного источника. Для смены К используйте процедуру Copy-Paste.

Если радиостанция не поддерживает шифрование, можно, сняв галочку 'Запись SSCK в радио', выполнить только обновление ключа К, используемого для аутентификации.

Параметр 'Текущий SCK Subset' позволяет назначить 10 ключей SCK как текущие (Current) и заменить, таким образом, активные ключи в KAG, работающие в разговорных группах на передачу.

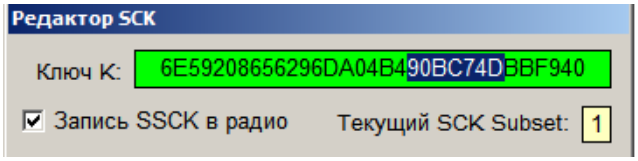
Каждый из ключей SCK можно редактировать или загрузить их набор из файла, выполнив 'Импорт SCK'.

Для выполнения записи ключей K и SSCK в радиостанцию нажмите 'Запись в радио'.

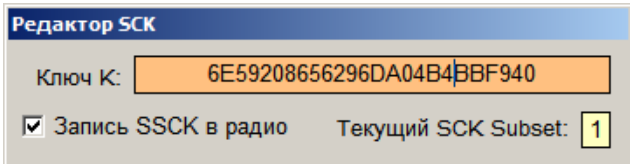
Редактирование и запись ключа К

Ключи аутентификации и шифрования можно записывать в любую радиостанцию вне зависимости от того, способна или нет она работать с шифрованием радиоинтерфейса.

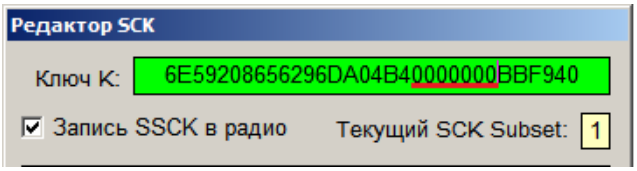
Для редактирования значения ключа К выделите его часть, подлежащую замене:



Нажмите 'Delete':

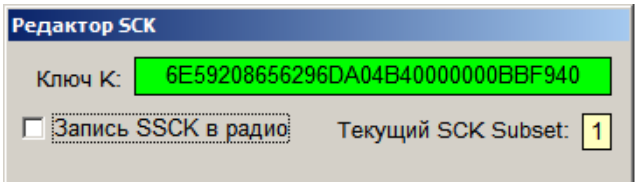


Вводите нужные данные в HEX-формате до достижения ключом длины 128 бит:



Если нужно заменить предлагаемое программой значение ключа К на полученное из доверенного источника, выделите, полностью удалите старый ключ и вставьте новое значение.

При работе с радиостанцией, не поддерживающей шифрование, для ускорения процесса можно ограничиться записью в нее только ключа аутентификации К. Снимите галочку 'Запись SSCK в радио':

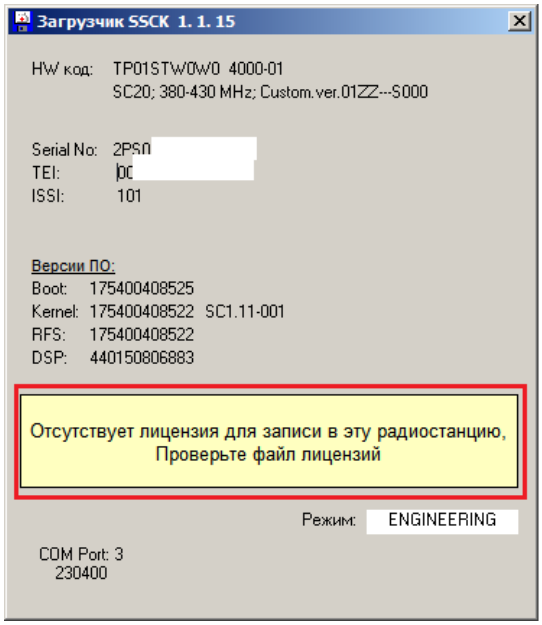


Когда ключ К имеет правильный формат, его значение подсвечивается зеленым фоном, и можно выполнять запись ключа К в радиостанцию. Запись К выполняется всегда первой, вне зависимости, будут ли далее записываться в радиостанцию ключи SCK или нет.

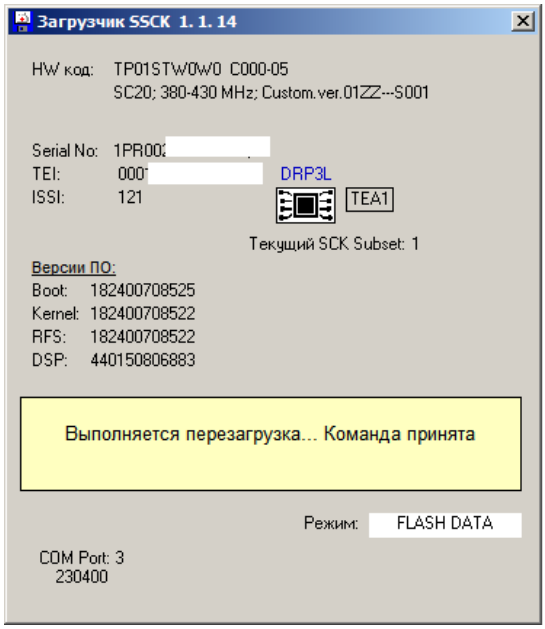
Для защиты от несанкционированного доступа к записи ключей в радиостанции служит лицензионный файл 'SSCK.lic', который должен размещаться в рабочей папке программы. Это текстовый документ, содержащий строки с парами TEI - Licence:

```
0001934593651710, Licence=C2D6403C589A77A66F0247736021C331
000370458701400, Licence=E2493327048695154E331A6120CAA07A
000109179542170, Licence=DB09E9C60997094A0D29AA4563F3B045
```

Нажмите 'Запись в радио'. Если в лицензионном файле отсутствует строка с лицензией для данной радиостанции, запись не выполняется и выводится сообщение об ошибке; радиостанция будет перезагружена:



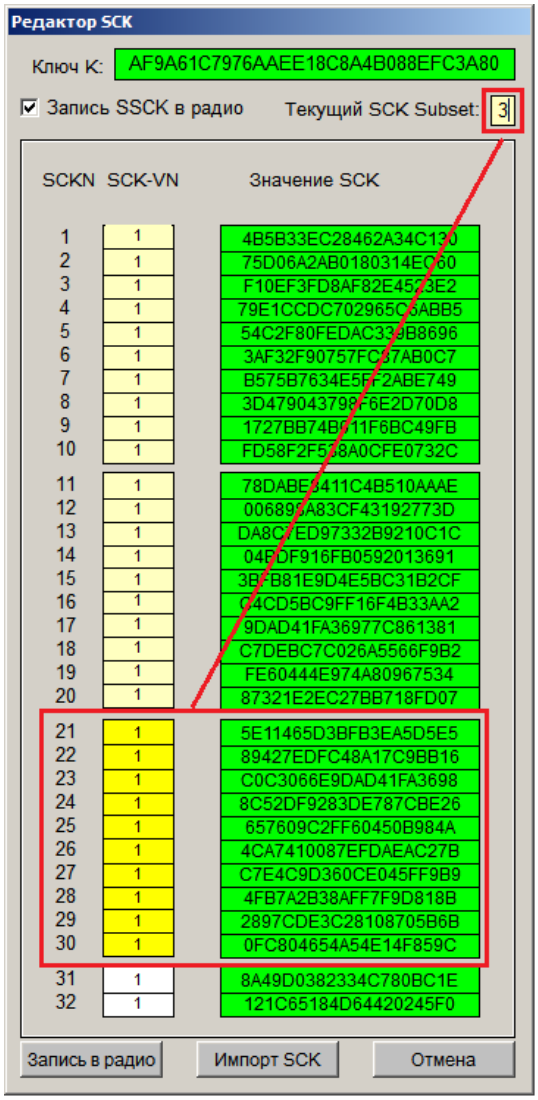
При наличии лицензии выполняется запись ключей в радиостанцию и, далее, ее перезагрузка:



Редактирование и запись номера SCK Subset

Вне зависимости от того, поддерживает ли радиостанция шифрование и включена ли опция записи ключей SSCK, всегда вместе с записью ключа K выполняется запись номера текущей подгруппы с активными на передачу ключами SCK.

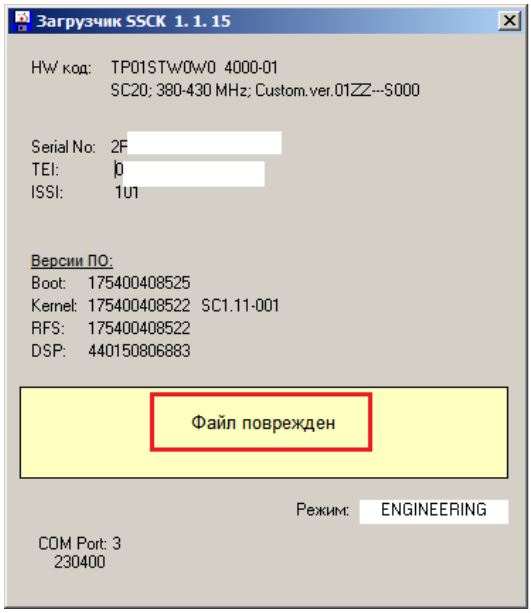
Введите нужный номер SCK Subset в диапазоне 1..3. При смене номера будет подсвечена подгруппа из 10 активных на передачу ключей SCK:



Редактирование ключей SCK и запись SSCK

Редактирование набора из 32-х ключей SCK доступно при включенной опции 'Запись SSCK в радио'. Помимо ручного редактирования предусмотрена возможность импорта готового набора ключей SCK из файла в формате SFPG01. Нажмите 'Импорт SCK' и выберите файл с данными для импорта.

При импорте файл проверяется на соответствие формату. В случае обнаружения ошибки выводится предупреждение и выполняется перезагрузка подключенной радиостанции:

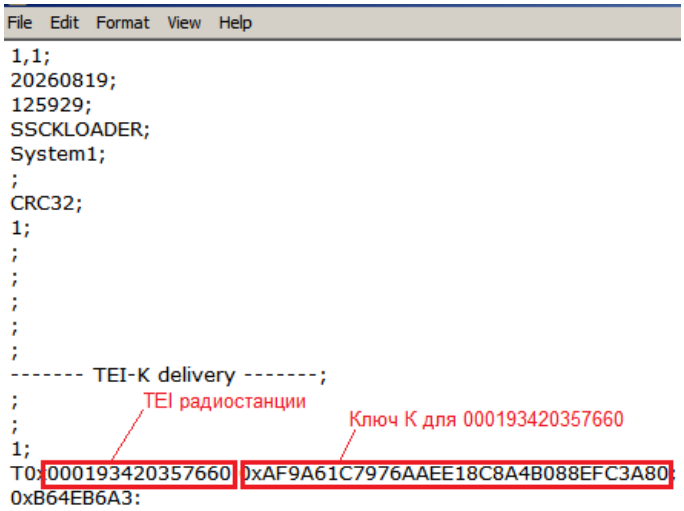


Помимо значений ключей SCK для редактирования доступны SCK-VN - номера версий ключей .
Когда все ключи SCK имеют правильный формат, их значения подсвечивается зеленым фоном, активируется кнопка 'Запись в радио' и можно выполнять запись ключей в радиостанцию.

Результаты выполнения программы

При успешном окончании каждого сеанса записи ключей в радиостанцию программа создает в своей рабочей папке файлы с результатами работы. Примеры:

Файл 'K for 000193420357660.txt' содержит TEI радиостанции и значение ее ключа аутентификации K.



Файл 'K for 000193420357660.txt'

Файл 'SCK_(Last Programmed).txt' содержит информацию о ключах SCK, использованных при последней записи ключей SSCK в радиостанцию. Наличие такого файла позволяет упростить запись аналогичного набора ключей SCK в другии радиостанции, выполнив предварительно его импорт.



Файл 'SCK_(Last Programmed).txt'

Файл 'SSCK for 000193420357660.txt' содержит список ключей SCK для радиостанции с TEI=000193420357660 в зашифрованном виде, что позволяет безопасно хранить и транспортировать данные, например в AuC SwMI.
Нужно отметить, что файл не содержит значения ключа K для данной радиостанции, что делает невозможной дешифровку значений SCK даже зная алгоритм получения SCK из SSCK.



Файл 'SSCK for 000193420357660.txt'

Параметр RSO, используемый для расчета SCK->SSCK при создании нового файла SSCK даже для одной и той же радиостанции, является случайным числом, следовательно, значения SSCK каждый раз будут различаться.

Не зная значения K невозможно выполнить дешифровку данных SSCK->SCK.

Безопасность

При работе по программированию ключей в радиостанции следует как можно больше внимание уделять вопросам обеспечения доступа на рабочем месте оператора и при хранении и транспортировке ключей.

Значение ключа K является основным секретом на котором построена вся система безопасности TETRA. Не менее важным является предотвращение утечки значений набора ключей шифрования SCK.

По окончании работы с программой сохраните и удалите с компьютера все созданные ею файлы с ключами K и SCK.