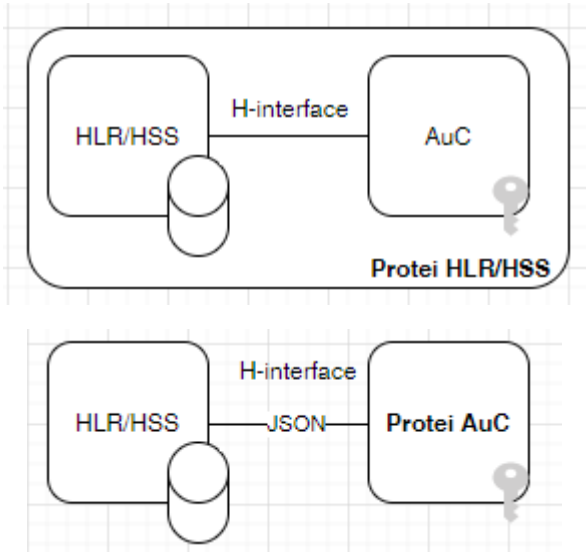
AuC аутентифицирует каждую SIM-карту (USIM/eUICC), которая пытается подключиться к сети мобильной связи. После успешной аутентификации HLR/HSS может управлять SIM-картой и предоставлять услуги абонентам. Также генерируется ключ шифрования, который впоследствии используется для шифрования всех беспроводных коммуникаций (голос, SMS и т. Д.) между мобильным телефоном и сетью GSM. Если аутентификация не прошла, то никакие услуги не будут доступны для этой конкретной комбинации SIM-карты и оператора мобильной связи.

Protei Authentication Centre (AuC) – это отечественный высокопроизводительный надежный центр аутентификации абонентов сотовой связи.

PROTEI AuC хранит учетные данные доступа (аутентификационную информацию) для каждого мобильного абонента, чтобы обеспечить аутентификацию и шифрование данных по радиоканалу между мобильной станцией и сетью. Процедура аутентификации включает в себя генерирование триплетов и квинтетов аутентификации.

PROTEI AuC хранит идентификационный ключ для каждого мобильного абонента вместе с параметрами алгоритма шифрования, которые могут отличаться для разных групп абонентов.

Модуль Protei_AuC может выступать как часть платформы Protei HLR/HSS, либо поставляться как standalone решение.



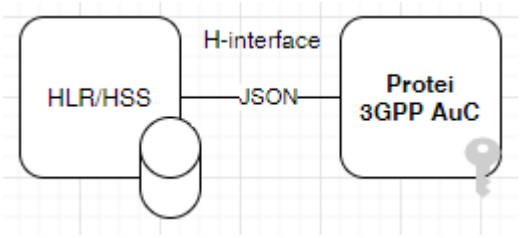
2. Варианты поставки

Protei AuC может поставляться в конфигурациях:

1. 3GPP AuC – с поддержкой алгоритмов аутентификации и шифрования, разработанных ассоциацией ETSI 3GPP.
2. HSM AuC – с поддержкой алгоритмов аутентификации и шифрования, рекомендованных российским законодательством.
3. 3GPP+HSM Auc – с поддержкой алгоритмов аутентификации и шифрования, разработанных ассоциацией 3GPP и алгоритмов аутентификации и шифрования, рекомендованных российским законодательством.

1.1 Protei 3GPP AuC

Protei 3GPP AuC может являться частью модуля HLR/HSS, либо взаимодействовать с ним посредством протокола JSON.



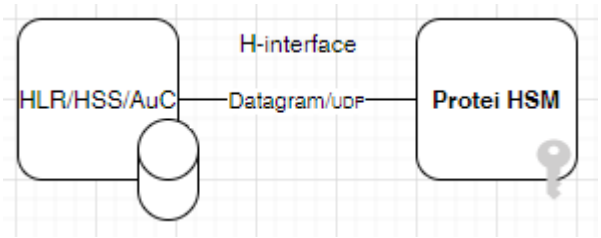
3GPP AuC реализует процедуры для аутентификации и шифрования, описанные в стандартах ETSI 3GPP:

- COMP 128 v2
- COMP 128 v3
- GSM Milenage (3GPP TS 55.205)
- Milenage (3GPP TS 35.205, 3GPP TS 35.206, 3GPP TS 35.207 и 3GPP TS 35.208.)
- TUAK (3GPP TS 35.231, 3GPP TS 35.232, 3GPP TS 35.233)

Все ключи могут храниться как в открытом, так и в зашифрованном виде. Для шифрования используются алгоритмы 3DES, DES и AES-128.

1.2 Protei HSM

Protei HSM взаимодействует с HLR/HSS, либо HLR/HSS/AuC по специально разработанному datagram протоколу.



Protei HSM реализован в соответствии с нормативными документами Российской Федерации:

- Приказ Минкомсвязи России от 27.06.2011 N 160 (ред. от 13.06.2018)

- рекомендации по стандартизации Р 1323565.1.003-2017.

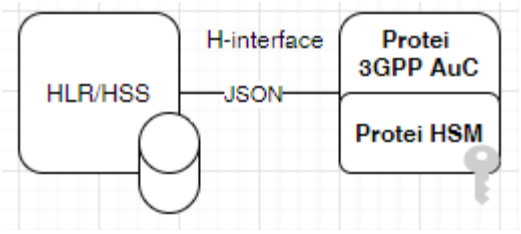
В модуле Protei HSM обеспечена поддержка алгоритмов шифрования S3G-128, S3G-256.

Все ключи могут храниться как в открытом, так и в зашифрованном виде. Для шифрования используются алгоритмы 3DES, DES и AES-128.

Хранение абонентских данных осуществляется на основе IMSI, либо Ki_ID. Возможно назначение различных алгоритмов шифрования разным группам абонентов.

1.3 Protei 3GPP HSM AuC

Protei 3GPP HSM AuC представляет из себя комбинацию 3GPP AuC и HSM. Взаимодействие с HLR/HSS осуществляется по протоколу JSON.



Возможно назначение различных алгоритмов шифрования разным группам абонентов.

3. Программно-аппаратная платформа

Protei AuC разворачивается на базе серверов аппаратной платформы x86, физических, либо виртуальных, в т.ч. отечественного производства, входящих в реестр Минпромторга (ТОРП).
В качестве операционной системы может использоваться доверенная операционная система отечественного производства Альт 8 СП, либо Linux Open Source OS(RHEL, CentOS, OEL).

4. Резервирование, масштабирование, пропускная способность

PROTEI AuC - это решение операторского класса, которое может масштабироваться горизонтально в соответствии с растущими требованиями оператора. Модульная структура системы обеспечивает высокую надежность и позволяет экономично масштабировать систему в соответствии с ростом использования услуг и требованиями оператора.

Если один модуль достигает своей максимальной пропускной способности, в конфигурацию системы добавляются дополнительные модули. Несколько подсистем могут работают в режиме разделения нагрузки.

Пропускная способность одного модуля составляет до 5000 TPS. Количество серверов, работающих в режиме разделения нагрузки, не ограничено.

5. Информация о сертификатах

Программное обеспечение Protei AuC зарегистрировано в реестре Минцифры в составе HLR/HSS:

Домашний регистр местоположения / регистр абонентских данных PROTEI HLR/HSS (Запись в реестре Минцифры №6182 (https://reestr.minsvyaz.ru/reestr/167432/), сертификат ОС-2-СПС-1020).

Программное обеспечение Protei AuC имеет сертификат ОС-2-СПС-1077.