конференция
РусКрипто

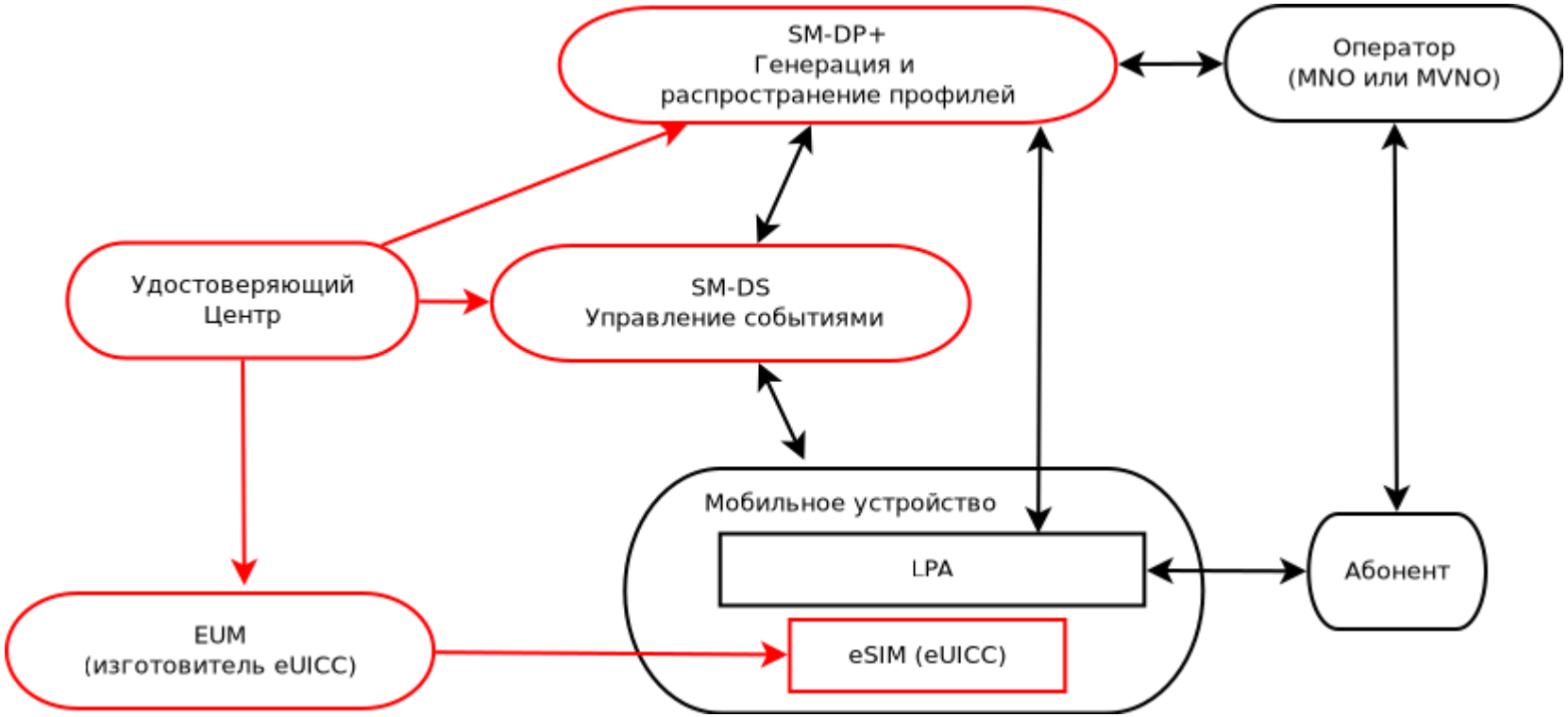
Ежегодная международная научно-практическая конференция

«РусКрипто'2022»

Особенности построения инфраструктуры PKI GSMA и оценка возможности создания российского аналога инфраструктуры PKI GSMA для его применения в российских экосистемах eSIM

Александров Сергей Викторович — технический директор,
Герасимова Алла Геннадьевна — рук. отд. системных исследований,
ООО «Системы практической безопасности»

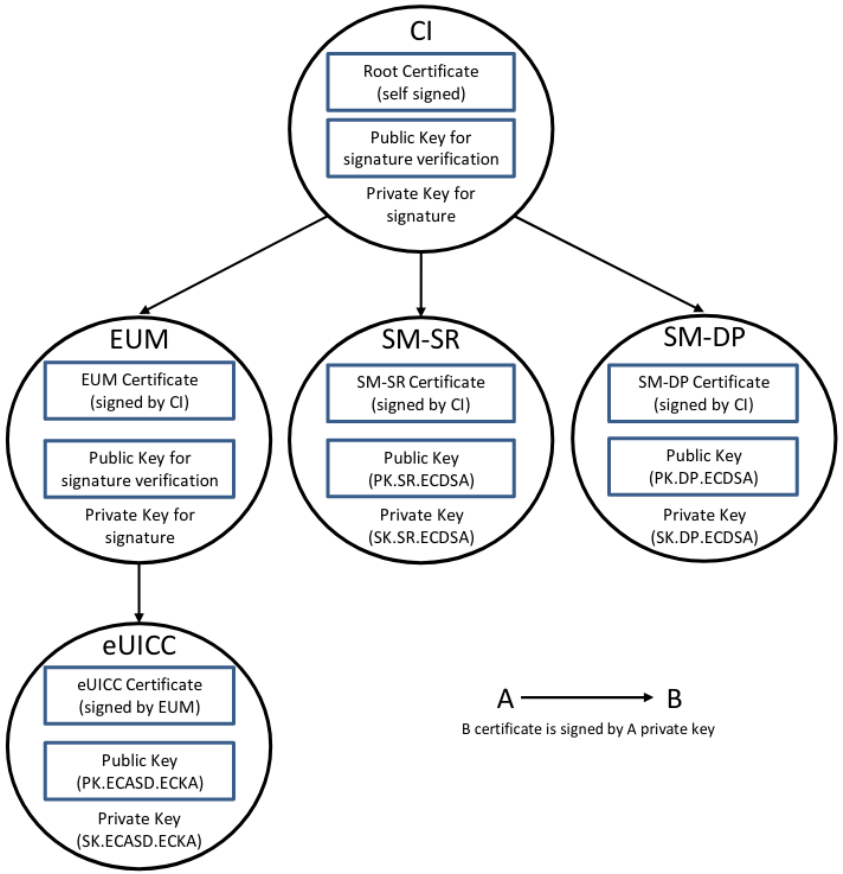
Общая архитектура GSMA



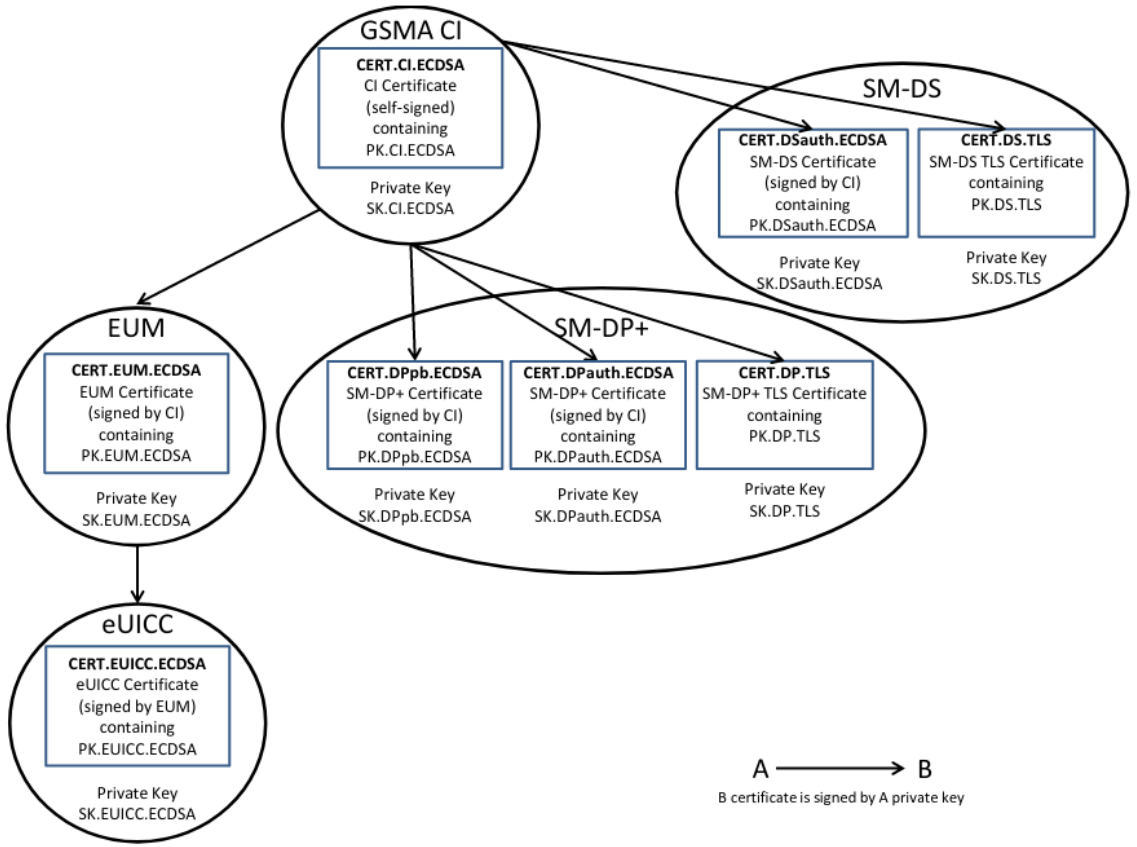
- Красным контуром выделены компоненты PKI GSMA

Инфраструктура PKI GSMA

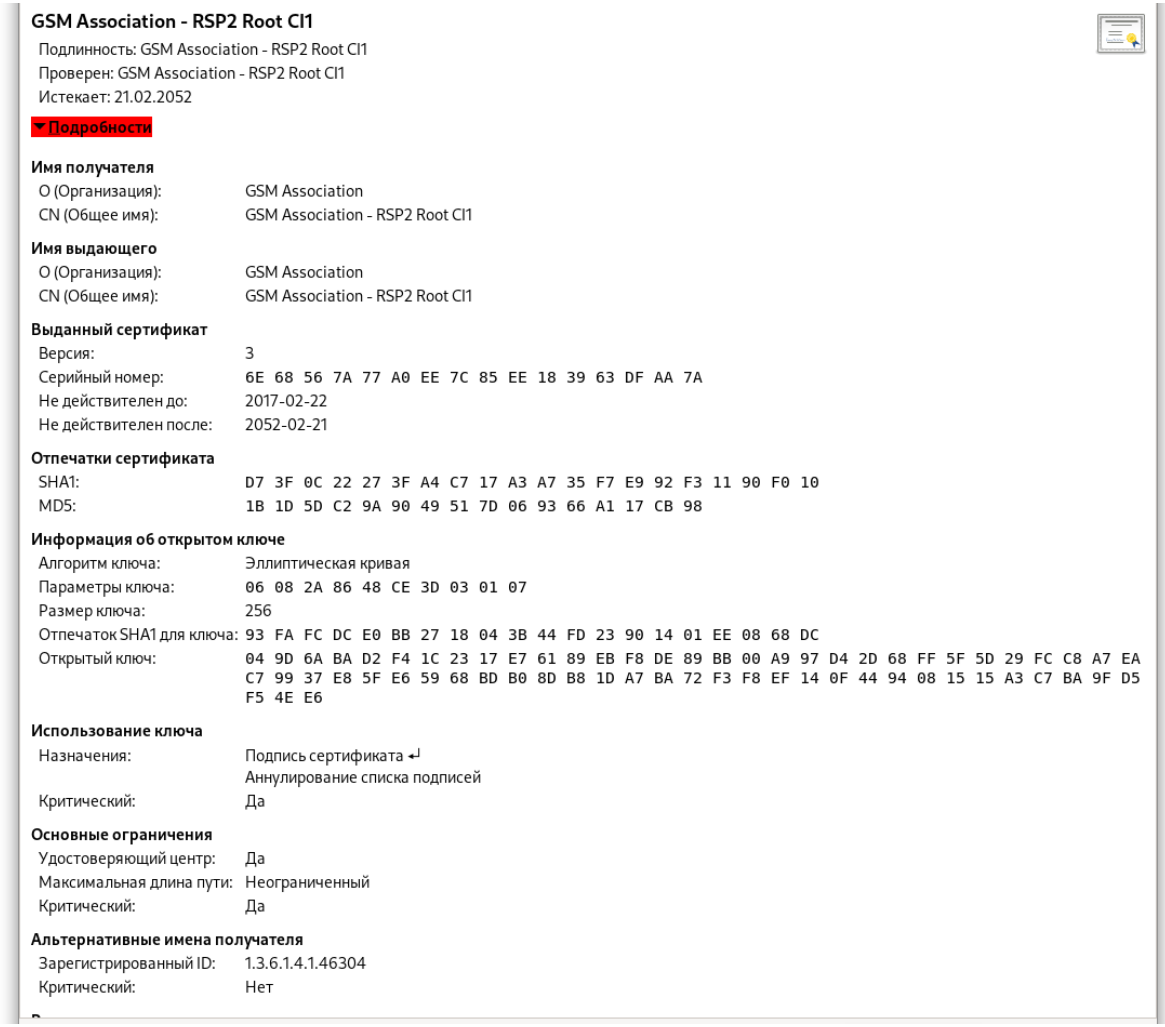
- M2M



- Consumer



Корневой сертификат PKI GSMA



GSM Association - RSP2 Root CI1

Подлинность: GSM Association - RSP2 Root CI1
Проверен: GSM Association - RSP2 Root CI1
Истекает: 21.02.2052

Подробности

Имя получателя

O (Организация):	GSM Association
CN (Общее имя):	GSM Association - RSP2 Root CI1

Имя выдающего

O (Организация):	GSM Association
CN (Общее имя):	GSM Association - RSP2 Root CI1

Выданный сертификат

Версия:	3
Серийный номер:	6E 68 56 7A 77 A0 EE 7C 85 EE 18 39 63 DF AA 7A
Не действителен до:	2017-02-22
Не действителен после:	2052-02-21

Отпечатки сертификата

SHA1:	D7 3F 0C 22 27 3F A4 C7 17 A3 A7 35 F7 E9 92 F3 11 90 F0 10
MD5:	1B 1D 5D C2 9A 90 49 51 7D 06 93 66 A1 17 CB 98

Информация об открытом ключе

Алгоритм ключа:	Эллиптическая кривая
Параметры ключа:	06 08 2A 86 48 CE 3D 03 01 07
Размер ключа:	256
Отпечаток SHA1 для ключа:	93 FA FC DC E0 BB 27 18 04 3B 44 FD 23 90 14 01 EE 08 68 DC
Открытый ключ:	04 9D 6A BA D2 F4 1C 23 17 E7 61 89 EB F8 DE 89 BB 00 A9 97 D4 2D 68 FF 5F 5D 29 FC C8 A7 EA C7 99 37 E8 5F E6 59 68 BD B0 8D B8 1D A7 BA 72 F3 F8 EF 14 0F 44 94 08 15 15 A3 C7 BA 9F D5 F5 4E E6

Использование ключа

Назначения:	Подпись сертификата Аннулирование списка подписей
Критический:	Да

Основные ограничения

Удостоверяющий центр:	Да
Максимальная длина пути:	Неограниченный
Критический:	Да

Альтернативные имена получателя

Зарегистрированный ID:	1.3.6.1.4.1.46304
Критический:	Нет

-----BEGIN CERTIFICATE-----
MIICSTCCAe+gAwIBAgIQbmhWeneg7nyF7hg5Y9+qejAKBggqhkjOPQQDAjBEMRgw
FgYDVQQKEw9HU00gQXNzb2NpYXRpb24xKDAmBgNVBAMTH0dTTSBBc3NvY2lhdGlv
biAtIFJTUDIgUm9vdCBDSTEwIBcNMTcwMjIyMDAwMDAwWhgPMjA1MjAyMjEyMzU5
NTlaMEQxGDAWBgNVBAoTD0dTTSBBc3NvY2lhdGlvbjEoMCYGA1UEAxMfR1NNIEFz
c29jaWF0aW9uIC0gUlNQMiBSb290IENJMTBZMBMGByqGSM49AgEGCCqGSM49AwEH
A0IABJ1qutL0HCMX52GJ6/jeibsAqZfULWj/X10p/Min6seZN+hf5llovbCNuB2n
unLz+O8UD0SUCBUVo8e6n9X1TuajgcAwgb0wDgYDVR0PAQH/BAQDAgEGMA8GA1Ud
EwEB/wQFMAMBAf8wEwYDVR0RBAwwCogIKwYBBAGC6WAwFwYDVR0gAQH/BA0wCzAJ
BgdngRIBAgEAME0GA1UdHwRGMEQwQqBAoD6GPGh0dHA6Ly9nc21hLWNybC5zeW1h
dXRoLmNvbS9vZmZsaW5lY2EvZ3NtYS1yc3AyLXJvb3QtY2kxLmNybDAdBgNVHQ4E
FgQUgTcPUSXQsdQI1MOyMubSXnlb6/swCgYIKoZIzj0EAwIDSAAwRQIgIJdYsOMF
WziPK7l8nh5mu0qiRiVf25oa9ullG/OIASwCIQDqCmDrYf+GziHXBOiwJwnBaeBO
aFsiLzIEOaUuZwdNUw==
-----END CERTIFICATE-----

Сертификаты PKI GSMA

Сертификаты используются для аутентификации объекта с помощью подписи, созданной с использованием ECDSA, а также для согласования ключей при установлении защищенного TLS-соединения.

Рекомендовано использование одной из следующих эллиптических кривых:

- NIST P-256, определенная в стандарте цифровой подписи [NIST SP 800-56A];
- brainpoolP256r1, определенная в RFC 5639;
- FRP256V1, определенный в ANSSI ECC [ANSSI ECC FRP256V1].

Алгоритм и параметры подписи:

Ecdsa-with-SHA256 (RFC 5758 и RFC 5759);

Поле 'AlgorithmIdentifier.parameters' должно отсутствовать.

Есть требования к наличию политик сертификата для каждый сущности:

Например, расширение 'Certificate Policies' должно быть установлено в OID 'id-rspRole-euicc' для сертификата eUICC, OID 'id-rspRole-eum' для сертификата EUM и т.д.

Варианты построения инфраструктуры открытых ключей для российской экосистемы eSIM (локализация PKI)

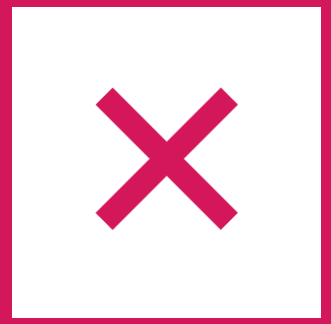
1) PKI-инфраструктура GSMA с зарубежными криптоалгоритмами (аналог действующей PKI-инфраструктуры GSMA на российском сегменте);

2) PKI-инфраструктура GSMA с российскими криптоалгоритмами (в случае включения российских криптографических алгоритмов в перечень рекомендованных и стандартизированных GSMA);

3) Гибридная PKI-инфраструктура с российскими и зарубежными криптоалгоритмами (поддержка одновременно двух PKI инфраструктур (российской и GSMA), каждая во главе со своим корневым удостоверяющим центром);

4) Российская национальная PKI-инфраструктура с российскими криптоалгоритмами, независимая от GSMA (автономная PKI-инфраструктура со своим корневым удостоверяющим центром).

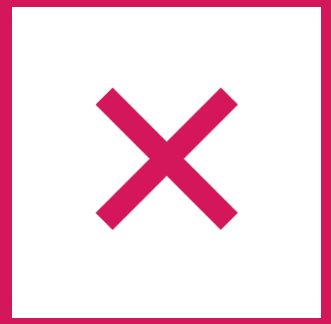
PKI-инфраструктура GSMA с зарубежными криптоалгоритмами (использование существующих решений)



- Использование исключительно зарубежных криптографических алгоритмов, содержащих потенциальные уязвимости, несущие риски раскрытия и/или подмены ключей абонентов
- Необходимость получения сертификатов GSMA и связанные с этим риски их отзыва

- Не требуется доработок - использование готовых изделий "под ключ"

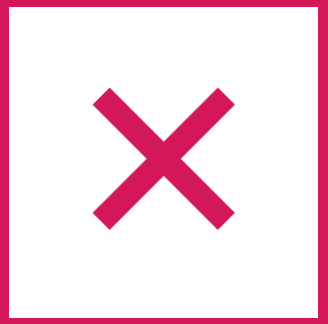
PKI-инфраструктура GSMA с российскими криптоалгоритмами
(включение российских криптографических алгоритмов в перечень рекомендованных и стандартизированных GSMA)



- Сложная и длительная процедура легализации российских криптографических алгоритмов в GSMA
- Необходимость получения сертификатов GSMA и связанные с этим риски их отзыва
- Разработка или модернизация всех компонентов RSP-платформы для внедрения российских криптографических алгоритмов

- Легализация российских криптографических алгоритмов в международной системе стандартизации GSMA
- Обеспечение безопасной загрузки абонентских профилей в МУ с eUICC на территории РФ
- Возможность загрузки абонентских профилей как российских, так и зарубежных мобильных операторов

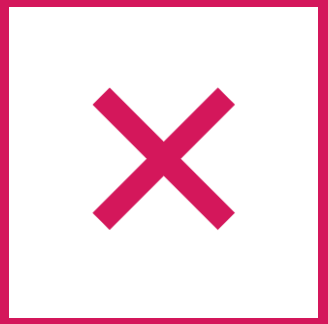
Гибридная PKI-инфраструктура с российскими и зарубежными криптоалгоритмами
(одновременная поддержка двух PKI инфраструктур)



- Необходимость разворачивания национальной PKI, дублирующей весь набор сертификатов GSMA
- Необходимость получения сертификатов GSMA
- Разработка или модернизация всех компонентов RSP-платформы для внедрения российских криптографических алгоритмов

- Возможность автономного функционирования платформы RSP в условиях отзыва сертификатов GSMA
- Обеспечение безопасной загрузки абонентских профилей в МУ с eUICC на территории РФ
- Возможность загрузки абонентских профилей как российских, так и зарубежных мобильных операторов
- Нет необходимости внедрять отечественные алгоритмы в стандарты GSMA

Российская национальная PKI-инфраструктура независимая от GSMA
(полностью российское решение)



- Отсутствие возможности загрузки абонентских профилей в доверенные МУ с российской eUICC за пределами РФ
- Отсутствие возможности загрузки абонентских профилей в МУ с eUICC зарубежного производства на территории РФ
- Разработка или модернизация всех компонентов RSP-платформы для внедрения российских криптографических алгоритмов

- Отсутствие необходимости получения сертификатов GSMA
- Обеспечение безопасной загрузки абонентских профилей в МУ с eUICC на территории РФ
- Нет необходимости внедрять отечественные алгоритмы в стандарты GSMA

Варианты локализации PKI - сравнение

	PKI GSMA с зарубежными криптоалгоритмами	PKI GSMA с отечественными криптоалгоритмами	Гибридная PKI инфраструктура	Российская национальная PKI инфраструктура
Загрузка профиля с отечественного SM-DP+ на МУ с отечественной eSIM	Да	Да	Да	Да
Загрузка профиля с зарубежного SM-DP+ на МУ с отечественной eSIM	Да	Да	Да	Нет
Загрузка профиля с отечественного SM-DP+ на МУ с зарубежной eSIM	Да	Да	Да	Нет
Аутентификация МУ с отечественной eSIM в РФ	Да	Да	Да	Да
Аутентификация МУ с отечественной eSIM в сети зарубежного оператора	Да	Да	Да	Нет, только роуминг
Аутентификация МУ с зарубежной eSIM в РФ	Да	Да	Да	Нет, только роуминг
Устойчивость на террритории РФ к отзыву сертификата GSMA CI	Нет	Нет	Да	Да

Выводы

Оптимальный вариант построения инфраструктуры открытых ключей для российской экосистемы eSIM - гибридная PKI-инфраструктура с российскими и зарубежными криптоалгоритмами, обеспечивающая:

- безопасную загрузку абонентских профилей в доверенные МУ с российской EUICC;
- стабильное функционирование RSP-платформы на территории РФ в условиях изоляции;
- отсутствие ограничений при использовании как абонентских профилей зарубежных МО в доверенных МУ с российской EUICC на пределами РФ, так и абонентских профилей российских МО в МУ с EUICC зарубежного производства на территории РФ.

Вопросы, требующие решения

???

Разработка ключевой системы и создание центра(ов) формирования КИ;

- Развёртывание инфраструктуры PKI во главе с корневым УЦ для RSP-платформы на территории РФ;
- Внедрение российской криптографии в протоколы доведения абонентских профилей;
- Разработка российской eUICC с реализацией российских и зарубежных алгоритмов и протоколов;
- Создание системы доверенной аутентификации абонентов, включая SM-DP, SM-DP+, SM-DS, HSS\HLR\AuC и т. д.;
- Доработка мобильных устройств с возможностью поддержки отечественных алгоритмов в TLS (опционально).

Вопросы

???

Контактная информация

Электронная почта:

aleksandrov@systempb.ru

geralla@systempb.ru

Телефон:

+ 7 (812) 468-15-61

Сайт:

www.systempb.ru