Приложение 2
к распоряжению Департамента
информационных технологий
города Москвы
от _____
№ _____

РЕГЛАМЕНТ
информационного взаимодействия посредством общегородского модуля регионального сегмента города Москвы государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных»

1. Общие положения

1.1. Настоящий Регламент информационного взаимодействия посредством общегородского модуля регионального сегмента города Москвы государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных» (далее – Регламент) определяет порядок взаимодействия посредством общегородского модуля регионального сегмента города Москвы государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных» (далее – ОМ РС ЕБС) при осуществлении аутентификации с использованием биометрических персональных данных физических лиц.

1.2. Регламент разработан в соответствии с постановлением Правительства Российской Федерации от 26 августа 2024 г. № 1151 «Об образовании регионального сегмента единой биометрической системы в г. Москве» (далее – Постановление № 1151), постановлением Правительства Москвы от 3 сентября 2024 г. № 1998-ПП «О региональном сегменте единой биометрической системы» и иными нормативными правовыми актами, регулирующими вопросы, которые затрагиваются настоящим Регламентом.

1.3. В Регламенте используются следующие термины, определения и сокращения:

1.3.1. Аутентификация – совокупность мероприятий по проверке физического лица на принадлежность ему идентификаторов с использованием биометрических персональных данных физического лица, векторов единой биометрической системы, реализуемых ОМ РС ЕБС.

1.3.2. БПД – биометрические персональные данные.

1.3.1. ГИС ЕБС – государственная информационная система «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных».

1.3.2. ДИТ – Департамент информационных технологий города Москвы;

1.3.3. Интерфейс взаимодействия – программный интерфейс взаимодействия с ОМ РС ЕБС.

1.3.4. ИС – информационная система, обеспечивающая оказание услуг (сервисов) с использованием РС ЕБС.

1.3.5. ОМ РС ЕБС – общегородской модуль регионального сегмента города Москвы ГИС ЕБС.

1.3.6. Оператор ОМ РС ЕБС– государственное казенное учреждение города Москвы «Московское городское агентство по телекоммуникациям».

1.3.7. Пользователь регионального сегмента города Москвы ГИС ЕБС (Пользователь РС ЕБС) – физическое лицо, взаимодействующее с РС ЕБС с целью размещения своих БПД в РС ЕБС, осуществления аутентификации с использованием БПД в РС ЕБС и в иных случаях.

1.3.8. Потребитель – орган исполнительной власти города Москвы, подведомственная ему организация, организация, созданная Правительством Москвы, органом исполнительной власти города Москвы либо подведомственной ему организацией, иная организация города Москвы, использующая ОМ РС ЕБС с целью аутентификации Пользователей.

1.3.9. Промышленная зона ОМ РС ЕБС – контур ОМ РС ЕБС, в котором обрабатываются данные Пользователей РС ЕБС и обеспечивается реализация информационного обмена для случаев, предусмотренных Постановлением № 1151.

1.3.10. Разработчик – лицо, являющееся производителем, разработчиком, правообладателем ИС или иное лицо, уполномоченное на взаимодействие в рамках настоящего Регламента.

1.3.11. РС ЕБС – региональный сегмент города Москвы ГИС ЕБС.

1.3.12. СКУД – система контроля и управления доступом.

1.3.13. СМКСС – средство мониторинга качества сопровождения систем.

1.3.14. СНИЛС – страховой номер индивидуального лицевого счета

1.3.15. СУДИР – автоматизированная информационная система «Система управления доступом к информационным системам и ресурсам города Москвы».

1.3.16. Терминал взаимодействия с Пользователем – аппаратное или программно-аппаратное средство Потребителя, оснащенное видеокамерой или веб-камерой, предназначенное для взаимодействия с Пользователем РС ЕБС в рамках реализации Потребителем услуг (сервисов) посредством аутентификации в ОМ РС ЕБС.

1.3.17. Тестовая зона ОМ РС ЕБС – выделенный контур, функционирующий аналогично промышленной зоне ОМ РС ЕБС, за исключением обработки персональных данных Пользователей РС ЕБС,

и который служит для отладки и проверки работоспособности взаимодействия ИС с ОМ РС ЕБС.

1.4. Участниками взаимодействия в соответствии с Регламентом являются:

1.4.1. Оператор ОМ РС ЕБС.

1.4.2. ДИТ.

1.4.3. Потребитель.

1.4.4. Разработчик.

1.5. Взаимодействие при осуществлении аутентификации с использованием БПД физических лиц осуществляется в случаях, предусмотренных нормативными правовыми актами Российской Федерации и города Москвы.

2. Общие сведения о взаимодействии ИС с ОМ РС ЕБС

2.1. Взаимодействие ИС с ОМ РС ЕБС осуществляется посредством интерфейса взаимодействия в соответствии с описанием, приведенным в Приложении 1 к настоящему Регламенту.

2.2. В рамках взаимодействия ИС с ОМ РС ЕБС Оператор ОМ РС ЕБС:

2.2.1. Предоставляет доступ ИС к ОМ РС ЕБС путем передачи авторизационных данных технологической учетной записи Потребителя в соответствии с Актом по форме в соответствии с приложением 2 к настоящему Регламенту.

2.2.2. Предоставляет техническую возможность использовать встраиваемый в Терминал взаимодействия с Пользователем программный компонент захвата кадров видеопотоков для передачи полученных кадров в ОМ РС ЕБС для целей аутентификации.

2.2.3. Осуществляет прием и обработку в ОМ РС ЕБС фотоизображений или видеопотоков, полученных с камер Терминалов взаимодействия с Пользователем или камер видеонаблюдения, установленных в контрольно-пропускных пунктах Потребителя для целей аутентификации.

2.2.4. Обеспечивает проведение аутентификации Пользователей РС ЕБС, информация о которых предварительно предоставлена Потребителем в РС ЕБС посредством интерфейса взаимодействия, и направляет информацию о результатах аутентификации посредством интерфейса взаимодействия.

2.2.5. Вправе анализировать действия ИС в рамках взаимодействия с ОМ РС ЕБС в целях оптимизации работы ОМ РС ЕБС и (или) взаимодействия ИС с ОМ РС ЕБС, а также для осуществления статистического учета.

2.2.6. Ведет технологический мониторинг информационного обмена ИС Потребителя и ОМ РС ЕБС для целей обеспечения бесперебойной работы ОМ РС ЕБС.

2.2.7. Вправе приостановить или прекратить информационный обмен между ОМ РС ЕБС и ИС Потребителя в случаях, когда запросы ИС Потребителя создают угрозу нарушения функционирования ОМ РС ЕБС, РС ЕБС или иных информационных системы и ресурсов города Москвы.

2.2.8. Обеспечивает консультационную поддержку Потребителя при направлении Потребителем обращений в порядке, определенном Оператором ОМ РС ЕБС в сроки, не превышающие 15 (пятнадцати) рабочих дней.

2.3. В рамках взаимодействия с ОМ РС ЕБС Потребитель:

2.3.1. Обеспечивает техническую готовность ИС Потребителя к интеграции и взаимодействию с ОМ РС ЕБС.

2.3.2. Обеспечивает использование в ИС Потребителя программных и технических средств СКУД, интегрированных с ОМ РС ЕБС.

2.3.3. Обеспечивает автоматическую передачу в ОМ РС ЕБС видеопотока, кадров видеопотоков, фотоизображений, а также иной информации, предусмотренной интерфейсом взаимодействия ОМ РС ЕБС, для целей аутентификации.

2.3.4. Обеспечивает обработку в ИС Потребителя результатов аутентификации, полученных из ОМ РС ЕБС.

2.3.5. Обеспечивает выполнение мер информационной безопасности в соответствии с разделом 5 настоящего Регламента.

2.3.6. Обеспечивает консультационную поддержку Пользователя РС ЕБС при осуществлении аутентификации в порядке и сроках, определенных Потребителем или соглашениями между Потребителем и Пользователем РС ЕБС.

2.4. Взаимодействие СКУД с ОМ РС ЕБС осуществляется в соответствии с пунктами 2.1 – 2.3 настоящего регламента.

2.5. ДИТ обеспечивает консультационную поддержку и организационно-методического сопровождение Пользователей ОМ РС ЕБС при размещении биометрических персональных данных, в порядке и сроках, определенных ДИТ.

3. Порядок взаимодействия при тестировании решений СКУД

3.1. Программные и (или) аппаратные средства СКУД (далее – решения СКУД), использующие функции аутентификации, могут быть интегрированы с ОМ РС ЕБС в соответствии с настоящим Регламентом.

3.2. До проведения тестирования Разработчик осуществляет интеграцию решений СКУД, выполняющих функции аутентификации с использованием биометрических персональных данных, с ОМ РС ЕБС в соответствии с требованиями приложения 1 к настоящему Регламенту.

3.3. Проведение тестирования интеграции решений СКУД с ОМ РС ЕБС производится на основании заявки Разработчика по форме приложения 3 к настоящему Регламенту (далее – Заявка на тестирование).

3.4. Заявка на тестирование направляется Разработчиком Оператору ОМ РС ЕБС посредством электронной почты Оператора ОМ РС ЕБС, либо по адресу местонахождения Оператора ОМ РС ЕБС посредством почтовой связи, либо нарочно по адресу местонахождения Оператора ОМ РС ЕБС в рабочее время Оператора.

3.5. Оператор ОМ РС ЕБС рассматривает поданную Заявку на тестирование в течение 15 (пятнадцати) рабочих дней. О результатах

рассмотрения Заявки на тестирование Оператор ОМ РС ЕБС сообщает заявителю посредством электронной почты.

3.6. В случае отсутствия замечаний к Заявке на тестирование, Оператор ОМ РС ЕБС направляет заявителю реквизиты доступа к Тестовой зоне ОМ РС ЕБС.

3.7. При наличии замечаний к Заявке на тестирование, Оператор ОМ РС ЕБС направляет Заявителю замечания посредством электронной почты, указанной в Заявке на тестирование.

3.8. После устранения замечаний Разработчик повторно направляет заявку в адрес Оператора ОМ РС ЕБС.

3.9. Для тестирования Разработчик проводит подготовительные мероприятия по подключению решения СКУД посредством инфраструктуры Разработчика к Тестовой зоне ОМ РС ЕБС в соответствии с реквизитами доступа, направленными Оператором ОМ РС ЕБС.

3.10. После завершения подготовительных мероприятий Разработчик уведомляет Оператора ОМ РС ЕБС о готовности к проведению тестирования решения СКУД.

3.11. Оператор ОМ РС ЕБС организует проведение тестирования в течение 15 (пятнадцати) рабочих дней после получения уведомления от Разработчика.

3.12. Тестирование включает в себя проверку взаимодействия решения СКУД с ОМ РС ЕБС в части реализации следующей функциональности:

3.12.1. Создание и удаление профилей.

3.12.2. Обработка событий аутентификации.

3.12.3. Передача кадров с терминалов (панелей) СКУД.

3.12.4. Отображение результата аутентификации на терминале (панели) СКУД.

3.12.5. Иные функции по решению Оператора ОМ РС ЕБС.

3.13. По решению Оператора ОМ РС ЕБС тестирование может проводиться в формате демонстрации решения СКУД Разработчиком.

3.14. По результатам тестирования Оператор ОМ РС ЕБС принимает решение об успешности интеграции решения СКУД с ОМ РС ЕБС.

3.15. Оператор ОМ РС ЕБС публикует перечень решений СКУД, успешно интегрированных с ОМ РС ЕБС на сайте городской системы видеонаблюдения (Портал Правительства Москвы) по адресу https://video.dit.mos.ru.

3.16. Перечень решений содержит следующие сведения:

3.16.1. Вид решения СКУД.

3.16.2. Наименование Разработчика.

3.16.3. Адрес веб-сайта Разработчика.

3.16.4. Дата внесения решения СКУД в перечень.

3.16.5. Список функциональных возможностей решения СКУД, определенный Оператором ОМ РС ЕБС по результатам тестирования.

3.16.6. Иные сведения.

3.17. В случае, когда решение СКУД введено в эксплуатацию у Потребителя, по решению Оператора ОМ РС ЕБС испытания могут быть проведены в Промышленной зоне ОМ РС ЕБС.

4. Порядок взаимодействия при подключении ИС Потребителя к ОМ РС ЕБС

4.1. Подключение ИС Потребителя к ОМ РС ЕБС осуществляется на основании:

4.1.1. Письменной заявки на подключение ИС к ОМ РС ЕБС (далее – Заявка на подключение), направленной Потребителем официальным письмом в адрес ДИТ по форме согласно приложениям 4, 5 к настоящему Регламенту;

4.1.2. Заключенного соглашения об информационном и технологическом взаимодействии с Оператором ОМ РС ЕБС и ДИТ по форме согласно приложению 6 к настоящему Регламенту (далее – Соглашение).

4.2. Оператор ОМ РС ЕБС рассматривает поданные Заявки на подключение в течение 15 (пятнадцати) рабочих дней.

4.3. В случае отсутствия замечаний к Заявке на подключение, Оператор ОМ РС ЕБС:

4.3.1. Организует передачу сведений, необходимых для организации канала связи между ИС Потребителя и ОМ РС ЕБС в соответствие с разделом 5 настоящего Регламента.

4.3.2. Направляет Соглашение Потребителю для подписания.

4.4. Потребитель после получения от Оператора ОМ РС ЕБС сведений, предусмотренных пунктом 4.3.1 Регламента, организует канал связи между ИС Потребителя и ОМ РС ЕБС, соответствующий требованиям раздела 5 настоящего Регламента и подписывает Соглашение.

4.5. После подписания Соглашения об информационном и технологическом взаимодействии Оператор ОМ РС ЕБС предоставляет доступ ИС Потребителя к ОМ РС ЕБС путем передачи авторизационных данных технологической учетной записи в соответствии с формой Акта, являющейся приложением 2 к Регламенту.

4.6. Нормативными документами ДИТ могут устанавливаться иные формы Соглашений для отдельных видов ИС и (или) Потребителей.

4.7. При наличии замечаний к Заявке на подключение Оператор ОМ РС ЕБС, уведомляет об этом Потребителя посредством электронной почты, указанной в Заявке на подключение.

4.8. После устранения замечаний Потребитель повторно направляет Заявку на подключение в адрес Оператора ОМ РС ЕБС.

4.9. Подключение СКУД Потребителя к ОМ РС ЕБС осуществляется в соответствии с пунктами 4.1 – 4.8 настоящего регламента.

5. Информационная безопасность при взаимодействии с ОМ РС ЕБС

5.1. Взаимодействие ИС и (или) СКУД с ОМ РС ЕБС осуществляется по каналам связи, защищенным с использованием средств криптографической защиты класса КС3 (далее – каналы связи) в соответствии с приказом Минцифры России от 5 мая 2023 г. № 445 «Об утверждении перечня угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица в единой биометрической системе, а также актуальных при взаимодействии информационных систем государственных органов, органов местного самоуправления, Центрального банка Российской Федерации, организаций, за исключением организаций финансового рынка, индивидуальных предпринимателей, нотариусов с единой биометрической системой, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных».

5.2. Организация каналов связи осуществляется посредством криптошлюза VipNet Coordinator HW. Взаимодействие между Оператором ОМ РС ЕБС и Потребителем осуществляется посредством организации межсетевого взаимодействия.

5.3. Обмен информацией, необходимой для организации криптографического межсетевого взаимодействия (номера сетей, и иная), осуществляется между Оператором ОМ РС ЕБС и Потребителем в рабочем порядке до начала информационного взаимодействия. Оператор ОМ РС ЕБС передает Потребителю ключевую информацию посредством Акта приема-передачи ключевых носителей (приложение № 7 к Регламенту) по месту нахождения Оператора ОМ РС ЕБС. По завершении установления межсетевого взаимодействия Оператором ОМ РС ЕБС и Потребителем составляется Акт установления межсетевого взаимодействия по форме, приведенной в приложении № 8 к Регламенту.

5.4. В рамках информационного взаимодействия ИС и (или) СКУД с ОМ РС ЕБС Потребитель обязуется:

5.4.1. Определить требования по защите информации, предъявляемые ИС Потребителя в соответствии с нормативными правовыми актами Российской Федерации, в том числе с учетом требований приказов ФСТЭК России:

- от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (до 1 марта 2026 г.);
- от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» (с 1 марта 2026 г.);
- от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности

персональных данных при их обработке в информационных системах персональных данных».

5.4.2. Обеспечить выполнение требований приказа Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требованиям к защите персональных данных для каждого из уровней защищенности», а также приказа Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» в отношении средств криптографической защиты информации, установленных в информационной системе Стороны.

5.4.3. Выполнять требования по защите информации в соответствии с Федеральным законом от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации».

5.4.4. Направить Оператору ОМ РС ЕБС подтверждение выполнения мер по защите информации, определенных в соответствии с пунктом 5.4.1 Регламента, посредством электронной почты до начала взаимодействия.

5.4.5. Уведомлять Оператора ОМ РС ЕБС посредством электронной почты о возникновении угроз и фактах сбоя и (или) нарушения в работе, возникновении угроз и фактах утечки информации, а также о нарушениях требований по защите информации, которые могут привести к нарушению функционирования ИС (СКУД) Потребителя и (или) ОМ РС ЕБС, в течение 24 часов
с момента возникновения соответствующего события. Стороны имеют право временно приостановить информационное взаимодействие в зависимости от возможности влияния инцидента информационной безопасности на ИС (СКУД) Потребителя и (или) ОМ РС ЕБС. В случае приостановки информационного взаимодействия Стороны уведомляют друг друга в рабочем порядке.

Приложение 1
к Регламенту информационного взаимодействия посредством общегородского модуля регионального сегмента города Москвы государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных»

Описание программного интерфейса взаимодействия посредством общегородского модуля регионального сегмента города Москвы государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных»

1.Термины и определения

В описании программного интерфейса используются в том числе следующие термины с соответствующими определениями:

Термин	Определение
Идентификатор сервиса	Уникальная строка, идентифицирующая ИС Потребителя или СКУД Потребителя.
Профиль	Связка БПД Пользователя с Сервисом
Внешний провайдер аутентификации	Указание на способ задания идентификатора БПД для целей создания профиля. Перечень доступных для Сервиса внешних провайдеров аутентификации определяется на этапе подключения.
Метка доступа	Связка источника видео или фотоизображения с Сервисом.
Сервис	ИС Потребителя или СКУД Потребителя, подключенная к ОМ РС ЕБС.

2. Авторизация

2.1. Получение access токена и refresh токена

Запрос:

POST https://{host}:{port}/realms/t-ebs/protocol/openid-connect/token

Данные запроса:

Content-Type: application/x-www-form-urlencoded

Описание параметров запроса:

Параметр	Описание	Обязательность
client_id	Идентификатор сервиса	Да
client_secret	Пароль сервиса	Да
username	Логин технологической учетной записи	Да
password	Пароль технологической учетной записи	Да
grant_type	Вариант авторизации. Передаваемое значение: password	Да

Пример ответа:

```
{
   "access_token": "eyJhbGciOi.....",
   "expires_in": 7776000,
   "refresh_expires_in": 7776000,
   "refresh_token": "dafre4ygGBJ.....",
   "token_type": "Bearer",
   "not-before-policy": 1711359988,
   "session_state": "a2b9gdjd-dbjwh3jdj-srqi-sgdudnjdhdc",
   "scope": "profile email"
}
```

Описание параметров ответа:

Параметр	Описание	Обязательность
access_token	Access токен для выполнения запросов	Да
expires_in	Время жизни токена доступа	Да
refresh_ecpires_in	Время жизни refresh токена	Да
token_type	Тип токена. Значение по-умолчанию: Bearer	Да
not-before-policy	Служебное поле	Да
scope	Служебное поле	Да

Полученный access токен необходимо использовать во всех последующих запроса в заголовках HTTP в следующем формате:

Описание полей заголовков:

Параметр	Описание	Обязательность
JWT	Авторизационный токен	Да
X-ACS-ServiceId	Идентификатор сервиса	Да

2.2. Обновление access токена по refresh токен

Запрос:

POST https://{host}:{port}/realms/t-ebs/protocol/openid-connect/token

Данные запроса:

Content-Type: application/x-www-form-urlencoded

Описание параметров запроса:

Параметр	Описание	Обязательность
client_id	Идентификатор сервиса	Да
client_secret	Пароль сервиса	Да
grant_type	Способ авторизации. Передаваемое значение: refresh_token	Да
refresh_token	Раннее полученный refresh токен	Да

Пример ответа:

{
"access_token": "eyJhbGciOi.....",
"expires_in": 7776000,
"refresh_expires_in": 7776000,
"refresh_token": "dafre4ygGBJ.....",
"token_type": "Bearer",
"not-before-policy": 1711359988,
"session_state": "a2b9gdjd-dbjwh3jdj-srqi-sgdudnjdhdc",
"scope": "profile email"
}

Описание параметров ответа:

Параметр	Описание	Обязательность
access_token	Access токен для выполнения запросов	Да
expires_in	Время жизни токена доступа	Да
refresh_expires_in	Время жизни refresh токена	Да
token_type	Тип токена. Значение по-умолчанию: Bearer	Да
not-before-policy	Служебное поле	Да
scope	Служебное поле	Да

3. Управление профилями

3.1. Получение профилей сервиса

Запрос:

GET https://{host}:{port}/v1/profile

Описание query-параметров запроса:

Параметр	Описание	Обязательность
acs_profile_id	Идентификатор профиля пользователя в сервисе	Нет
service	Идентификатор сервиса	Нет
provider	Мнемоника внешнего провайдера аутентификации	Нет
sort	Сортировка по возрастанию и убыванию id. По умолчанию sort=id Возможные значения: -id, id	Нет
limit	Количество результатов в выдаче, максимум 10000, по-умолчанию 1000	Нет
page	Значение курсора страницы, полученное в поле 'next_page' в ответе	Нет

Пример ответа:


```
{
 "profiles": [
  {
   "acs_profile_id": "acs_profile_id",
   "service": "parsiv",
   "provider": "sudir",
   "provider_person_id": "string",
   "bio_registered": true
  }
 ],
 "nextPage": 0
}
```


Описание параметров ответа:

Параметр		Описание	Тип	Обязательность
profiles		Массив профилей	Array	Да
	acs_profile_id	Идентификатор профиля пользователя в сервисе	String	Нет
	service	Идентификатор сервиса	String	Нет
	provider	Мнемоника внешнего провайдера аутентификации	String	Нет
	provider_person_id	Идентификатор биометрии пользователя	String	Да
	bio_registered	Признак наличия биометрии	Boolean	Да
page		Идентификатор следующей страницы	String	Нет

3.2. Создание профилей сервиса

Запрос:

POST https://{host}:{port}/v1/profile

Пример запроса:

```
{
 "profiles": [
  {
   "service": "parsiv",
   "acs_profile_id": "acs_profile_id",
   "provider": "sudir",
   "provider_person_id": "string"
  }
 ]
}
```

Описание параметров запроса:

Параметр		Описание	Тип	Обязательность
profiles		Массив профилей	Array	Да
	acs_profile_id	Идентификатор профиля пользователя в сервисе	String	Да
	service	Идентификатор сервиса	String	Да
	provider	Мнемоника внешнего провайдера аутентификации	String	Да
	provider_person_id	Идентификатор биометрии пользователя	String	Да

Пример ответа:

```
{
 "profiles": [
  {
   "acs_profile_id": "acs_profile_id",
   "service": "parsiv",
   "provider": "sudir",
   "provider_person_id": "string",
   "bio_registered": true
  }
 ]
}
```

Описание параметров ответа:

Параметр		Описание	Тип	Обязательность
profiles		Массив профилей	Array	Да
	acs_profile_id	Идентификатор профиля пользователя в сервисе	String	Нет
	service	Идентификатор сервиса	String	Нет

	provider	Мнемоника внешнего провайдера аутентификации	String	Нет
	provider_person_id	Идентификатор биометрии пользователя	String	Да
	bio_registered	Признак наличия биометрии	Boolean	Да

3.3. Удаление профиля сервиса

Запрос:

DELETE https://{host}:{port}/v1/profile/{acs_profile_id}

Описание параметров запроса:

Параметр	Описание	Тип	Обязательность
acs_profile_id	Идентификатор профиля	String	Да

Описание query-параметров запроса:

Параметр	Описание	Тип	Обязательность
service	Идентификатор сервиса	String	Да

В случае успешности данные ответа пустое, http-код – 204.

4. Управление листами доступа

4.1. Добавление меток сервиса в лист доступа

Запрос:

POST https://{host}:{port}/v1/access

Пример запроса:

```
{
 "label_values": [
  "gate",
  "foo",
  "bar"
 ]
}
```

Описание параметров запроса:

Параметр	Описание	Тип	Обязательность
label_values	Метки доступа, по которым определяется принадлежность события аутентификации к сервису	Array	Да

Пример ответа:

```
{
 "label_values": [
  "gate",
```

```
   "foo",
   "bar"
 ]
}
```

Описание параметров ответа:

Параметр	Описание	Тип	Обязательность
label_values	Метки доступа, по которым определяется принадлежность события аутентификации к сервису	Array	Да

4.2. Получение меток сервиса в листе доступа

Запрос:

GET https://{host}:{port}/v1/access

Пример ответа:

```
{
 "label_values": [
   "gate",
   "foo",
   "bar"
 ]
}
```

Описание параметров ответа:

Параметр	Описание	Тип	Обязательность
label_values	Метки доступа, по которым определяется принадлежность события аутентификации к сервису	Array	Да

4.3. Удаление меток сервиса из листа доступа

Запрос:

DELETE https://{host}:{port}/v1/access

Пример ответа:

В случае успешного ответа возвращается http-код 200.

5. Получение сообщений о событиях аутентификации из брокера сообщений

Авторизация в брокере сообщений выполняется посредством SASL с токеном, полученным с помощью методов из п. 2.

Пример сообщения в брокере сообщений:

```
{
  "label_value": string,
  "acs_profile_ids": [string],
  "timestamp": string,
  "camera": string,
  "acs_service_id": string,
  "session_id": string,
  "auth_status": "success"
}
```

Описание параметров сообщения:

Параметр	Описание	Тип	Обязательность
acs_profile_ids	Идентификатор профиля	String	Нет
timestamp	Дата и время события	String	Да
camera	Идентификатор камеры	String	Да
label_value	Значение метки сервиса в листе доступа	String	Да
acs_service_id	Идентификатор сервиса	String	Да
session_id	Идентификатор сессии в случае его передачи во время запроса на аутентификацию	String	Нет
auth_status	Результат аутентификации: «success» - успешная аутентификация, «failed» - неуспешная аутентификация, «error» - ошибка в процессе аутентификации.	String	Да

6. Передача фотоизображений с терминалов взаимодействия с пользователем

Фотоизображения с терминалов взаимодействия с пользователем передаются в брокер сообщений.

Пример сообщения в брокере сообщений в формате MsgPack с JSON:

```
{
  "camera_id": "31ad1ce7-74b5-4220-9ca8-8c0e27cac0ed",
  "created_at": "2024-05-05T11:33:12+03:00",
  "labels": {
    "ebs": "ebs",
    "acs_test-service": "test-label"
  },
```

"photo": <набор байт>
}

Описание параметров сообщения:

Параметр	Описание	Тип	Обязательность
camera_id	Идентификатор терминала взаимодействия с пользователем	String	Да
created_at	Дата и время формирования фотоизображения	String	Да
labels	Набор меток для аутентификации	JSON Object	Да
ebs	Метка, определяющая принадлежность фотоизображения к РС ЕБС. Значение по умолчанию – ebs	String	Да
acs_test-service	Метка, определяющая принадлежность фотоизображения к сервису, при этом: test-service – значение идентификатора сервиса test-label – метка, сформированная сервисом в листе доступа	String	Да
photo	Фотоизображение в виде набора байт	ByteArray	Да

Приложение 2
к Регламенту информационного взаимодействия посредством общегородского модуля регионального сегмента города Москвы государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных»

Форма

Акт передачи авторизационных данных технологической учетной записи к общегородскому модулю регионального сегмента города Москвы государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных» (ОМ РС ЕБС)

г.Москва «___»_____ 20__г.

1. ГКУ «Мосгортелеком») (Оператор ОМ РС ЕБС) в лице _____ *(ФИО, должность)* предоставил технологический доступ к ОМ РС ЕБС для целей интеграции _____ *(наименование ИС Потребителя)*, посредством передачи Авторизационных данных технологической учетной записи (далее – Авторизационные данные), а _____ *(наименование Потребителя)*, в лице_____*(ФИО, должность)* далее по тексту – Потребитель, принял указанную информацию, согласно таблице:

Таблица

N п/п	ФИО	Авторизационные данные

2. Настоящим Потребитель подтверждает, что:

2.1. Уведомлен о том, что Авторизационные данные, являются информацией ограниченного доступа и не подлежат разглашению и передаче третьим лицам и обязуется не передавать такую информацию третьим лицам.

2.2. Уведомлен, что несет ответственность в соответствии с действующим законодательством Российской Федерации за разглашение информации ограниченного доступа.

3. Настоящий акт составлен в двух экземплярах по одному для каждой из Сторон, имеющих одинаковую юридическую силу.

Передал документы: Принял документы:

_____ _____ _____ _____ _____ _____

(должность) (подпись) (ФИО) *(должность) (подпись) (ФИО)*

Приложение 3
к Регламенту информационного взаимодействия посредством общегородского модуля регионального сегмента города Москвы государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных»

Форма

ЗАЯВКА
на тестирование интеграции решения СКУД с общегородским модулем регионального сегмента города Москвы государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных»
(ОМ РС ЕБС)

«__» _____ 20___ г.

Заявитель:

полное наименование организации

сведения о государственной регистрации в качестве юридического лица или индивидуального предпринимателя

адрес местонахождения

телефон, факс, адрес веб-сайта, адрес электронной почты

в лице

должность, ФИО руководителя организации

просит рассмотреть возможность тестирования Решения СКУД

наименование и версия Решения СКУД

на предмет интеграции с ОМ РС ЕБС.

Ответственное лицо со стороны Заявителя:

ФИО

адрес электронной почты, номер телефона

ФИО ответственного лица

Приложения к заявке:

1. Документы, подтверждающие правомочия Заявителя в отношении программного обеспечения.

Руководитель организации

ФИО, подпись

М.П.

Приложение 4
к Регламенту информационного взаимодействия посредством общегородского модуля регионального сегмента города Москвы государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных»

Форма

Заявка
на подключение информационной системы (ИС) к общегородскому модулю регионального сегмента города Москвы государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных» (ОМ РС ЕБС)

Заявитель _____ *(наименование потребителя),* в лице _____*(должность, ФИО)* в соответствии с Регламентом информационного взаимодействия посредством общегородского модуля регионального сегмента города Москвы государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных» просит провести мероприятия по подключению ИС Потребителя к ОМ РС ЕБС в целях организации/осуществления _____ *(указываются цели использования РС ЕБС в рамках случаев использования РС ЕБС, установленных ПП РФ №1151)* и направляет схемы осуществления аутентификации с использованием биометрических персональных данных в рамках взаимодействия с ОМ РС ЕБС.

Приложения к заявке:

1. Описание реализации аутентификации с использованием биометрических персональных данных в рамках взаимодействия с ОМ РС ЕБС в виде схемы алгоритма, диаграммы последовательности или в ином виде.

Наименование ИС, подключаемой к ОМ РС ЕБС:

_____

Наименование организации:

_____

Место нахождения:

_____

_____

Контактная информация Потребителя:

_____

(ФИО, должность, эл.почта, телефон)

ИНН _____,

КПП _____,

ОГРН _____,

_____

(должность)

_____

(наименование Потребителя)

_____ _____

М.П. *(Фамилия И.О.)*

Приложение 5
к Регламенту информационного взаимодействия посредством общегородского модуля регионального сегмента города Москвы государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных»

Форма

Заявка
на подключение системы контроля и управления доступом (СКУД) к общегородскому модулю регионального сегмента города Москвы государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных» (ОМ РС ЕБС)

Заявитель _____ *(наименование потребителя),* в лице _____*(должность, ФИО)* в соответствии с Регламентом информационного взаимодействия посредством общегородского модуля регионального сегмента города Москвы государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных» просит провести мероприятия по подключению СКУД, находящихся на территории Потребителя (далее – объект) к ОМ РС ЕБС и направляет схемы организации прохода на объект, а именно: размещение контрольно-пропускных пунктов, размещение средств видеофиксации или фотофиксации, с указанием направления прохода (вход или выход), а также сведения в соответствии с приложением № 1 к настоящей заявке.

Приложения к заявке:

1. Сведения об объекте и состав технических средств СКУД в табличной форме.

2. Схемы организации прохода на объект, включая размещение контрольно-пропускных пунктов и средств видеофиксации или фотофиксации.

Наименование организации:

_____

Место нахождения:

_____

_____

Контактная информация Потребителя:

_____

(ФИО, должность, эл.почта, телефон)

ИНН _____,

КПП _____,

ОГРН _____,

_____

(должность)

_____

(наименование Потребителя)

_____ _____

М.П. *(Фамилия И.О.)*

Приложение к заявке на подключение системы контроля и управления доступом (СКУД) к общегородскому модулю регионального сегмента города Москвы государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных» (ОМ РС ЕБС)

Сведения
об объекте и состав технических средств СКУД

Сведения для подключения к ОМ РС ЕБС						
N п/п	Наименование объекта	Адрес объекта	Средства видеофиксации (перечень с указанием наименований камер, интегрированных с государственной информационной системой «Единый центр хранения и обработки данных», далее - ЕЦХД)	Средства фотофиксации (перечень с указанием производителей и моделей)	Средства управления СКУД в составе аппаратных устройств и программных средств (перечень с указанием производителей и моделей)	Средства обеспечения защиты информации (модель используемого оборудования, номер сети VipNet)
1	2	3	4	5	6	7

Примечания:

1. *В графе 4 указываются видеокамеры, интегрированные с ЕЦХД и установленные на контрольно-пропускных пунктах, предназначенные для реализации аутентификации*
2. *В графе 6 указываются средства управления СКУД, совместимые с ОМ РС ЕБС.*
3. *Графа 7 заполняется в случае, когда с ИС Потребителя ранее установлено межсетевое взаимодействие.*

Приложение 6
к Регламенту информационного взаимодействия посредством общегородского модуля регионального сегмента города Москвы государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных»

Форма

Соглашение
об информационном и технологическом взаимодействии между Департаментом информационных технологий города Москвы, Государственным казенным учреждением города Москвы «Московское городское агентство по телекоммуникациям» и _____*(наименование Потребителя)* при аутентификации физических лиц посредством общегородского модуля регионального сегмента города Москвы государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных»

г.Москва «___» _____ 2025 г.

Департамент информационных технологий города Москвы, в лице_____*(должность, ФИО)*, действующего*(ей)* на основании _____*(доверенность, НПА, иное)*, (далее – ДИТ), Государственное казенное учреждение города Москвы «Московское городское агентство по телекоммуникациям», в лице_____*(должность, ФИО)*, действующего*(ей)* на основании_____*(доверенность, Устав, иное)* (далее – ГКУ «Мосгортелеком»), и _____ *(наименование Потребителя)*, в лице _____*(должность, ФИО)*, действующий*(ая)* на основании _____*(доверенность, НПА, иное)*, и совместно именуемые в дальнейшем «Стороны», заключили Соглашение о нижеследующем.

1. ПРЕДМЕТ СОГЛАШЕНИЯ

1.1. Предметом Соглашения является информационное и технологическое взаимодействие Сторон в целях обеспечения аутентификации физических лиц

с использованием биометрических персональных данных, реализуемой РС ЕБС.

1.2. В рамках реализации Соглашения Стороны осуществляют информационное и технологическое взаимодействие при использовании ОМ РС ЕБС и _____*(указывается наименование ИС потребителя)* (далее – ИС Потребителя) в целях организации/осуществления _____ *(указываются цели использования РС ЕБС в рамках случаев использования РС ЕБС, установленных ПП РФ №1151).*

1.3. В настоящем Соглашении используются термины и определения, содержащиеся в Регламенте информационного взаимодействия посредством общегородского модуля регионального сегмента города Москвы государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных» (далее - Регламент, утвержден распоряжением ДИТ от ____ № _____).

2. УСЛОВИЯ ВЗАИМОДЕЙСТВИЯ СТОРОН

2.1. В рамках реализации Соглашения ГКУ «Мосгортелеком»:

2.2. Предоставляет доступ ИС Потребителя к ОМ РС ЕБС путем передачи авторизационных данных технологической учетной записи в соответствии с формой Акта, являющейся приложением к настоящему Соглашению.

2.3. Обеспечивает функционирование ОМ РС ЕБС.

И/Или

Предоставляет Потребителю техническую возможность использовать встраиваемый в Терминал взаимодействия с пользователем программный компонент захвата кадров видеопотоков для передачи полученных кадров в ОМ РС ЕБС для целей аутентификации.

И/Или

Осуществляет прием и обработку в ОМ РС ЕБС фотоизображений или видеопотоков, полученных с камер Терминалов взаимодействия с пользователем или камер видеонаблюдения, установленных в контрольно-пропускных пунктах Потребителя для целей аутентификации.

2.4. Обеспечивает проведение аутентификации в отношении Пользователей РС ЕБС, информация о которых предоставлена Потребителем в РС ЕБС посредством интерфейса взаимодействия, и направляет информацию о результатах аутентификации посредством интерфейса взаимодействия.

2.5. Вправе анализировать действия ИС Потребителя в рамках взаимодействия с ОМ РС ЕБС в целях оптимизации работы ОМ РС ЕБС и (или) взаимодействия ИС Потребителя с ОМ РС ЕБС.

2.6. Ведет технологический мониторинг информационного обмена ИС Потребителя и ОМ РС ЕБС для целей обеспечения бесперебойной работы ОМ РС ЕБС.

2.7. Вправе приостановить или прекратить информационный обмен между ОМ РС ЕБС и ИС Потребителя в случаях, когда запросы ИС Потребителя создают угрозу нарушения функционирования ОМ РС ЕБС, РС ЕБС или иных информационных системы и ресурсов города Москвы. О факте приостановления или прекращения информационного обмена, ГКУ «Мосгортелеком» уведомляет Потребителя в рабочем порядке.

2.8. Обеспечивает консультационную поддержку Потребителя путем обработки обращений, направленных Потребителем в ГКУ «Мосгортелеком» в сроки, не превышающие 15 (пятнадцати) рабочих дней.

2.9. В рамках реализации Соглашения Потребитель:

2.9.1. Обеспечивает техническую готовность ИС Потребителя к интеграции и взаимодействию с ОМ РС ЕБС.

Или

Обеспечивает использование в ИС Потребителя программных и технических средств систем контроля и управления доступом, совместимых с ОМ РС ЕБС. [1]

2.9.2. Осуществляет автоматическую передачу в ОМ РС ЕБС видеопотока, кадров видеопотоков, фотоизображений, а также иной информации, предусмотренной интерфейсом взаимодействия ОМ РС ЕБС, для целей аутентификации.

2.9.3. Обеспечивает обработку в ИС Потребителя результатов аутентификации, полученных из ОМ РС ЕБС, при реализации целей, установленных пунктом 1.2 Соглашения.

2.10. ДИТ, при необходимости, оказывает консультационную поддержку и организационно-методическое сопровождение Потребителю.

2.11. Стороны имеют право направлять друг другу запросы в любых формах и получать ответы на указанные запросы в установленные в них сроки.

3. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

3.1. Любая информация, предоставленная одной Стороной другой Стороне в рамках настоящего Соглашения, считается информацией ограниченного доступа и не подлежит разглашению или передаче третьим лицам без согласования с передающей Стороной.

3.2. Потребитель и ГКУ «Мосгортелеком» обязуются:

---

[1] Реестр программных и технических средств, совместимых с ОМ РС ЕБС, размещается Департаментом информационных технологий города Москвы в сети «Интернет» по адресу: https://video.dit.mos.ru/docs_rsebs/

3.2.1. Назначить ответственное лицо за информационную безопасность и направить его контактные данные на электронную почту другой Стороны для оперативного взаимодействия в случае инцидентов информационной безопасности. Электронная почта ГКУ «Мосгортелеком» – oib_video@it.mos.ru, электронная почта _____ - _____.

3.2.2. Организовать криптографическую защиту каналов связи с использованием средств криптографической защиты класса КС3 в соответствии с приказом Минцифры России от 5 мая 2023 г. № 445 «Об утверждении перечня угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица в единой биометрической системе, а также актуальных при взаимодействии информационных систем государственных органов, органов местного самоуправления, Центрального банка Российской Федерации, организаций, за исключением организаций финансового рынка, индивидуальных предпринимателей, нотариусов с единой биометрической системой, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных». Организация канала связи осуществляется посредством криптошлюза VipNet Coordinator HW. Обмен информацией, необходимой для организации криптографического межсетевого взаимодействия (номера сетей и иная), осуществляется в рабочем порядке. ГКУ «Мосгортелеком» передает Потребителю ключевую информацию посредством Акта приема-передачи ключевых носителей (приложение 7 к Регламенту). По завершении установления межсетевого взаимодействия Стороны подписывают Акт установления межсетевого взаимодействия по форме, приведенной в Приложении 8 к Регламенту.

3.3.3. Уведомлять друг друга посредством электронной почты, в сроки указанные в п. 5.4.3. Регламента, о возникновении угроз и фактах сбоя и (или) нарушения в работе, возникновении угроз и фактах утечки информации, а также о нарушениях требований по защите информации, которые могут привести к нарушению функционирования информационных систем Сторон.

3.3.4. Незамедлительно принять меры по устранению нарушений требований по защите информации, которые могут привести к утечкам информации (неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват) и (или) нарушению функционирования информационных систем Сторон.

3.4. Потребитель обязуется:

3.4.1. Направить ГКУ «Мосгортелеком» подтверждение выполнения мер по защите информации, установленных определенных нормативными правовыми актами Российской Федерации, в том числе приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите

информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (до 1 марта 2026 г.), от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» (с 1 марта 2026 г.) и Приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» посредством электронной почты до начала взаимодействия.

3.5. В рамках исполнения Соглашения сведения, составляющие государственную тайну, не обрабатываются.

4. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

4.1. Стороны договорились, что вопросы по урегулированию разногласий, возникающих в связи с толкованием и реализацией Соглашения, будут рассматриваться путем проведения переговоров и консультаций.

4.2. Соглашение вступает в силу с момента его подписания Сторонами и действует в течение одного года. Если любая из Сторон не заявила о прекращении действия Соглашения до момента прекращения срока его действия, определенного настоящим пунктом Соглашения, Соглашение подлежит автоматическому продлению на следующий год, с момента истечения его срока действия. Данный порядок продления срока действия Соглашения применятся ежегодно.

4.3. Любая из Сторон вправе в одностороннем порядке расторгнуть настоящее Соглашение путем направления соответствующего письменного уведомления другим Сторонам не менее чем за 30 рабочих дней до предполагаемой даты расторжения настоящего Соглашения.

4.4. Действие настоящего Соглашения прекращается с даты, указанной в уведомлении, но не ранее чем через 30 рабочих дней со дня направления Сторонам соответствующего уведомления.

4.5. В случае расторжения Соглашения обязательства Сторон, установленные разделом 2 Соглашения, прекращаются, если иное не предусмотрено законодательством Российской Федерации.

4.6. В настоящее Соглашение могут вноситься изменения и дополнения путем оформления дополнительных соглашений, являющихся неотъемлемыми частями Соглашения.

4.7. Соглашение составлено в 3 (трех) экземплярах, по одному для каждой из Сторон, имеющих одинаковую юридическую силу.

Департамент информационных технологий города Москвы

Адрес юридического лица:
123112, г.Москва, 1-й Красногвардейский пр-д, д.21, стр.1
Фактический (почтовый) адрес:
105064, г.Москва, Яковоапостольский пер., д.12, стр.1

ГКУ Мосгортелеком

Адрес юридического лица:
121059, г. Москва, ул. 1-я Бородинская ул., д.2А,

_____
(наименование Потребителя)

Адрес юридического лица:
_____

Фактический (почтовый) адрес:
_____

ПОДПИСИ СТОРОН:

_____
(должность)

Департамента информационных технологий города Москвы

_____ _____
М.П. *(Фамилия И.О.)*

_____
(должность)

ГКУ «Мосгортелеком»

_____ _____
М.П. *(Фамилия И.О.)*

_____
(должность)

_____
(наименование Потребителя)

_____ _____
М.П. *(Фамилия И.О.)*

Приложение 7
к Регламенту информационного взаимодействия посредством общегородского модуля регионального сегмента города Москвы государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных»

Форма

Акт
приема-передачи ключевых носителей

1. **Государственное казенное учреждение города Москвы «Московское городское агентство по телекоммуникациям»** (Оператор ОМ РС ЕБС), в лице ответственного пользователя СКЗИ _____*(ФИО, должность*) передал, а ответственный представитель _____*(наименование Потребителя),* в лице _____(ФИО, должность), далее именуемый «Получатель», принял для подключения ViPNet сети _____к ViPNet сети Оператора ОМ РС ЕБС _____ ключевые носители _____,

(номер ключевого носителя) содержащие следующие криптографические ключи:

- _____.lzh;
- _____.key.

2. Получатель обязуется предоставить Оператору ОМ РС ЕБС в течении 15 календарных дней согласованный акт Установления межсетевого взаимодействия между сетями (в двух экземплярах).

3. В случае непредоставления акта Установления межсетевого взаимодействия между сетями в установленный срок доступ приостанавливается.

4. Настоящий Акт составлен в двух экземплярах. Один экземпляр настоящего Акта хранится у ответственного пользователя СКЗИ, другой - у ответственного сотрудника.

Ответственный пользователь СКЗИ
_____ _____, «__» _____, 20__г.
(подпись)

Ответственный представитель
_____ _____, «__» _____, 20__г.
(подпись)

Приложение 8
к Регламенту информационного взаимодействия посредством общегородского модуля регионального сегмента города Москвы государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных»

Форма

Акт
Установления межсетевого взаимодействия между сетями

г. Москва «__» _____20__г.

Государственное казенное учреждение города Москвы «Московское городское агентство по телекоммуникациям» (Оператор ОМ РС ЕБС) в лице _____*(ФИО, должность),* действующего на основании _____, с одной стороны, и _____*(наименование Потребителя),* в лице _____*(ФИО должность*), действующий на основании, _____, с другой стороны, далее совместно именуемые Стороны, в соответствии с Регламентом информационного взаимодействия с общегородским модулем регионального сегмента города Москвы государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных» подписали настоящий акт о следующем:

Межсетевое взаимодействие установлено между ViPNet-сетями:

Номер ViPNet-сети	Наименование Потребителя

1. Целью установления межсетевого взаимодействия является защищенное информационное взаимодействие сетевых узлов ViPNet-сетей Оператора ОМ РС ЕБС и _____ *(наименование Потребителя)*.
2. Передача начального и ответного экспорта между ViPNet-сетями _____ и _____ была осуществлена доверенным способом.
3. Для установления межсетевого взаимодействия использовался _____ (указывается тип) межсетевой мастер-ключ, созданный в сетях ГКУ «Мосгортелеком».
4. Для установления межсетевого взаимодействия, в качестве шлюзовых ViPNet-Координаторов были определены:

- _____;
- _____;

(номер сети, наименование СКЗИ, версия ПО)

5. Смена межсетевых ключей, изменение состава сетевых узлов, участвующих в межсетевом взаимодействии, производится после предварительного согласования средствами взаимного экспорта/импорта, о чем технические специалисты Сторон уведомляют

друг друга посредством электронной почты в рабочем порядке с указанием производимых изменений.

6. В случае компрометации ключевой информации Стороны незамедлительно уведомляют друг друга посредством электронной почты в рабочем порядке, осуществляют временное приостановление информационного взаимодействия до момента последующей смены ключевой информации в соответствии с эксплуатационной документацией на криптографическое средство защиты информации.

7. Стороны обязуются производить изменения в настройках и структуре ViPNet-сетей, которые могут привести к нарушению межсетевого взаимодействия, только после предварительного согласования с другой Стороной в рабочем порядке.

Государственное казенное учреждение города Москвы «Московское городское агентство по телекоммуникациям»

ИНН 7701944546
КПП 773001001
Юридический адрес:
ул. 1-я Бородинская, д.2А,
г.Москва, 121059

_____
(наименование Потребителя)

ИНН _____
КПП _____

Юридический адрес:
_____
_____

ПОДПИСИ СТОРОН:

_____	_____
(должность)	*(должность)*
ГКУ «Мосгортелеком»	_____
	(наименование Потребителя)
_____ _____	_____ _____
М.П. *(Фамилия И.О.)*	М.П. *(Фамилия И.О.)*