№ вопроса	Пункт документации	Вопрос
1	-	Пожалуйста, сформулируйте цели и назначение системы ИА? Какие задачи и/или проблемы должна решать эта система? Цели и задачи указаны в главах 1.4 и 1.5 пункта 27 «Технические требования на выполнение ОКР по лоту 1». Назначение сервисов ИС – обеспечить ведение пользователей облачной платформы, их идентификацию и аутентификацию при доступе к сервисам облачной платформы. Судя по требуемой функциональности ИА можно отнести к классу Identity Manager. Исследовался ли вопрос внедрения готовых средств? Если «да», то почему эти средства не походят? В основе решения по сервисам ИА допустимо использовать элементы готовых средств или одно готовое средство при условии что решение по сервисам ИА будет соответствовать предъявляемым к нему техническим требованиям.
2	3.1.1 Регистрация пользователей Сервис ИА должен обеспечивать возможность регистрации пользователей на основании следующего минимального набора данных: адрес электронной почты; пароль. Для успешного завершения процесса регистрации пользователя сервис ИА должен требовать подтверждения пользователем своего адреса электронной почты. Подтверждение должно выполняться с помощью кода подтверждения, отправляемого на указанный при регистрации адрес электронной почты. Сервис ИА не должен требовать подтверждения других данных, указанных пользователем при регистрации. После успешного завершения процесса регистрации пользователь должен иметь возможность: успешно пройти аутентификацию, используя свой логин и пароль; войти в свой профиль, чтобы просмотреть, отредактировать и дополнить свои данные.	Какого назначение этого функционала? Зачем нужно пользователю регистрироваться в какой-то системе? К чему он в последствии должен получить доступ? В последствии пользователь должен иметь возможность получить доступ к любым сервисам облачной платформы, которые должны будут использовать сервис ИА для идентификации и аутентификации пользователей. Информация по текущим существующим сервисам облачной платформы присутствует на сайте облачной платформы Ростелеком – www.o7.com. Должно быть создано средство, обеспечивающее информационную и технологическую поддержку процесса подключения ИС к сервису ИА (Технологический портал).

3	3.1.2 Просмотр и редактирование данных пользователя Пользователь должен иметь возможность войти в свой профиль после того как успешно пройдѐ т аутентификацию в системе. В своѐ м профиле пользователь должен иметь следующие возможности: просмотреть и отредактировать свои личные и контактные данные (идентификационные данные), как минимум – ФИО, дату рождения, пол, адрес электронной почты, телефон. просмотреть и отредактировать данные, которые используются для аутентификации (аутентификационные данные), как минимум – логин и пароль; узнать текущий уровень достоверности идентификации и повысить его; узнать перечень организаций, в которые пользователь включѐ н; зарегистрировать организацию; удалить свою учѐ тную запись.	Как будет решаться вопрос о защите персональных данных? Как предполагается получать разрешение у пользователя на обработку его перс. данных? В рамках данных работ по созданию Опытного образца сервиса идентификации и аутентификации для облачной платформы согласно техническим требованиям не предусмотрены работы по защите персональных данных. В последующих работах должны быть обеспечены меры по защите персональных данных. Каковы требования к хранению перс. данных – требуется ли предусматривать средства шифрования? Каким требованиям они должны соответствовать? Специальные требования к хранению персональных данных в «Технических требованиях…» не специфицированы. Применение созданных в рамках работ в процессе опытной эксплуатации и в последствии сервисов ИА не должно приводить к нарушению действующего законодательства РФ в области обеспечения защиты персональных данных.
4	3.1.3 Регистрация организаций Сервис ИА обеспечивать возможность регистрации организации (создания учетной записи организации) на основании следующего минимального набора данных: полное наименование организации; должностное лицо, ответственное за ведение профиля организации в системе (администратора профиля организации).	Каково назначение этого функционала? Зачем нужно регистрировать организации и вести их профиль? Кто эти потенциальные «организации», которые будут это делать? Для сервисов облачной платформы, предназначенных для использования пользователями организаций необходимо иметь возможность при идентификации и аутентификации с использованием сервисов ИА получить информацию о пользователе как участнике определенной организации. Потенциальные организации – это организации-потребители сервисов облачной платформы. Регистрация организаций как-то связана с регистрацией пользователей? Пользователь – это всегда сотрудник какой-то организации? Или пользователь может быть сам по себе? Возможны обе категории пользователе – пользователь-физическое лицо и пользователь-сотрудник организации.

5	3.1.5 Применение парольных политик Сервис ИА должен предоставлять возможность настройки следующих парольных политик: требования к длине и сложности пароля; требования к сроку действия пароля. Сервис ИА должен проверять пароль на соответствие парольным политикам при создании и изменении пароля пользователем. Если пароль не соответствует парольным политикам, то Сервис ИА не должен позволять пользователю его назначить.	Больше политик не требуется? Только указанные? Дополнительные политики приветствуются.
6	3.1.6 Восстановление пароля пользователя Сервис ИА должен предоставлять пользователю возможность восстановления забытого пароля с использованием: подтверждения пользованием знания ответа на контрольный вопрос; мобильного телефона пользователя; электронной почты.	Просьба более подробно описать сценарий восстановления пароля по мобильному телефону – мы правильно понимаем, что пароль нужно SMSкой выслать? Или тут – мобильный телефон – как дополнительное средство идентификации пользователя? Должны быть доступны перечисленные в требовании возможности подтверждения личности пользователя в процессе восстановления пароля. При использовании мобильного телефона для подтверждения пароля возможны различные варианты – высылать пароль, высылать код восстановления и т.д. В предложениях конкурсанта хотелось бы увидеть отраженным его видение, как должна быть построена данная процедура.

7	3.2 Требования к функциям подсистемы аутентификации Подсистема аутентификации сервиса ИА должна обеспечить: возможность аутентификации пользователей на основе разовых паролей; интерфейс взаимодействия ИС с сервисом ИА в процессе идентификации и аутентификации пользователей; выделение уровней достоверности идентификации пользователей.	А зачем тогда нужен постоянный пароль, о котором идет речь в 3.1.5 и 3.1.6? Различные сервисы облачной платформы могут предъявлять различные требования к идентификации и аутентификации пользователей. Предоставьте, пожалуйста, технические требования к интерфейсу взаимодействия ИС и ВА Разработанный интерфейс взаимодействия ИС и сервисов ИА должен быть описан в техническом проекте и должен позволять обеспечить в соответствии с данным описанием взаимодействие сервисов облачной платформы с сервисами ИА при идентификации и аутентификации пользователей. Конкурсант может предложить свое видение того каким должен быть интерфейс взаимодействия. Пожалуйста, поясните, зачем это нужно? Какую задачу решает данный функционал? Сервисы ИА должны обеспечить возможность идентификации и аутентификации пользователей при доступе к сервисам облачной платформы в режимах, которые будут необходимы сервисам облачной платформы (по паролю, по разовому паролю)
8	3.2.1 Аутентификация пользователей на основе разовых паролей Сервис ИА должен обеспечивать возможность аутентификации пользователей с помощью разовых паролей, отправляемых пользователю в виде SMS-сообщения на номер мобильного телефона, указанного в профиле данного пользователя. Сервис ИА должен обеспечивать возможность отправки SMS-сообщения с разовым паролем на номер любого российского оператора сотовой связи посредством использования подсистемы уведомлений Системы обеспечения взаимодействия мобильных устройств с инфраструктурой электронного правительства. Срок действия разового пароля должен определяться настройками.	Что собой представляет «подсистема уведомлений Систему обеспечения взаимодействия мобильных устройств с инфраструктурой электронного пр-ва»? Можно ли получить требования к интерфесу с данной системой? Должна быть обеспечена возможность отправки SMS на мобильные устройства (телефоны). Интерфейс взаимодействия с подсистемой уведомления – web-сервисы (доступны по протоколу SOAP). Описание API подсистемы будут предоставлены победителю.
9	3.2.3 Поддержка уровней достоверности идентификации	Эти уровни присваивает человек или это автоматические процедуры? Присваивает сервис ИА на основе конкретных условий регистрации, идентификации и аутентификации пользователя.

10	3.2.3 Поддержка уровней достоверности идентификации 2. Уровень 2. Присваивается пользователям, личность которых подтверждена со стандартным уровнем гарантии (проверено реальное существование физического лица с помощью сервисов органов исполнительной власти, осуществляется подтверждение соответствия личности пользователя посредством отправки регистрируемого почтового отправления с кодом активации Почтой России или выдачи кода активации в центре регистрации). Для аутентификации используется логин и пароль.	Каким образом и с помощью каких конкретно сервисов будет осуществляться такая проверка? Конкурсант должен предложить варианты проверки. Существующие сервисы органов власти можно найти, например, на технологическом портале системы межведомственного электронного взаимодействия.
11	3.2.3 Поддержка уровней достоверности идентификации 3. Уровень 3. Присваивается пользователям, личность которых подтверждена с повышенным уровнем гарантии (проверено реальное существование личности при персональном посещении пользователем центра регистрации – офиса уполномоченной организации). Для аутентификации используется электронная подпись.	В требования к аутентификации нигде не упоминалась электронная подпись. Просьба пояснить в какой момент возникает это подпись? Как и где пользователь может получить сертификат для формирования такой подписи? Каким образом в момент аутентификации предполагается, что пользователь ее сформирует? Получение электронной подписи не входит в рамки данной работы. Нужно обеспечить идентификацию и аутентификацию с использованием электронной подписи, соответствующей законодательству РФ (63-ФЗ).
12	3.2.3 Поддержка уровней достоверности идентификации 4. Уровень 4. Присваивается пользователям (к ним, например, относятся пользователи с ролью должностного лица органа власти), регистрация и назначение полномочий которым выполнено уполномоченным сотрудником.	О каких полномочиях и на что идет речь? Категория сотрудников, которые регистрируются в органах власти – необходимо для сервисов облачной платформы, которые могут быть использованы сотрудниками государственных организаций. В качестве полномочий понимаются полномочия по доступу к облачным сервисам.