УТВЕРЖДАЮ
Генеральный директор
ООО «Кейсистемс»
_____ А. А. Матросов
«___» _____ 2022 г.

ПРОГРАММНЫЙ КОМПЛЕКС «ИНТЕГРАЦИЯ-КС»

ВЕРСИЯ 3.9

Руководство пользователя

Безопасность сервисной шины обмена сообщениями (Remote Messaging Service)

ЛИСТ УТВЕРЖДЕНИЯ

Р.КС. 09010-01 34 03-ЛУ

СОГЛАСОВАНО
Заместитель генерального директора
ООО «Кейсистемс»
_____ С. В. Панов
«___» _____ 2022 г.
Руководитель ДСР
_____ Д. Г. Пахомов
«___» _____ 2022 г.

2022

Литера А

Подп и дата	
Инв.N дубл	
Взам.инв.N	
Подп и дата	
Инв.N подл	

УТВЕРЖДЕНО
Р.КС. 09010-01 34 03-ЛУ

информационные технологии КЕЙСИСТЕМС

ПРОГРАММНЫЙ КОМПЛЕКС «ИНТЕГРАЦИЯ-КС»

ВЕРСИЯ 3.9

Руководство пользователя

Безопасность сервисной шины обмена сообщениями (Remote Messaging Service)

Р.КС. 09010-01 34 03

Листов 9

2022

Литера А

Подп и дата	
Инв.N дубл	
Взам.инв.N	
Подп и дата	
Инв.N подл	

АННОТАЦИЯ

Настоящий документ является частью руководства пользователя программного комплекса «Интеграция-КС» версии 3.9 от 01.03.2022 г. и содержит описание операций по администрированию сервиса обмена сообщениями RMS (Remote Messaging Service).

Руководство состоит их двух разделов:

- Описание операций.
- Рекомендации по освоению.

Раздел *«Описание операций»* содержит описание всех выполняемых функций, задач, описание операций по администрированию сервиса обмена сообщениями.

Раздел *«Рекомендации по* освоению*»* содержит рекомендации и разъяснения по использованию сервиса обмена сообщениями пользователем.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Настоящее руководство пользователя содержит описание администрирования сервиса обмена сообщениями программного комплекса «Интеграция-КС» (далее – «программный комплекс»).

Условные обозначения

В документе используются следующие условные обозначения:

 Уведомление	–	Важные сведения о влиянии текущих действий пользователя на выполнение других функций, задач программного комплекса.
 Предупреждение	–	Важные сведения о возможных негативных последствиях действий пользователя.
 Предостережение	–	Критически важные сведения, пренебрежение которыми может привести к ошибкам.
 Замечание	–	Полезные дополнительные сведения, советы, общеизвестные факты и выводы.
[Выполнить]	–	Функциональные экранные кнопки.
<F1>	–	Клавиши клавиатуры.
«Чек»	–	Наименования объектов обработки (режимов).
Статус	–	Названия элементов пользовательского интерфейса.
ОКНА => НАВИГАТОР	–	Навигация по пунктам меню и режимам.
п. 2.1.1 *рисунок 5*	–	Ссылки на структурные элементы, рисунки, таблицы текущего документа, ссылки на другие документы.

1. ОПИСАНИЕ ОПЕРАЦИЙ

Как известно, безопасность обеспечивается комплексом мер: административными, техническими, программными мерами пр. В данном документе рассматривается обеспечение безопасности на уровне самого сервиса.

Непроизвольно или специально RMS-сервис может быть доступен из вне, т.е. из сети Internet или Intranet. В таких случаях необходима защита, т.е. авторизованный доступ к его ресурсам и к механизму отправки/приема сообщений.

Аутентификация определяет - кто вошел в систему, под каким именем, а Авторизация – имеет ли данный пользователь права на те или иные ресурсы и операции. На уровне ASP.NET приложения, коим является RMS-сервис, аутентификация включается/отключается в файле Web.config:

```
<system.web>
   <!-- Аутентификация: None, Forms -->
   <authentication mode="Forms">
      <forms loginUrl="~/admin.ashx/Login" timeout="2880" />
   </authentication>
 …
</system.web>
```

При режиме аутентификации отличном от **None**, любой http запрос к RMS-сервису проходит проверку на наличие специального токена безопасности. Дальнейшее поведение системы зависит от реализации механизма авторизации на уровне конкретного запрашиваемого ресурса.

У сервиса две внешних точки доступа, через которые происходит основное обращение к ресурсам:

- admin.ashx;
- Точка входа Web-администратора сервиса.
- service.ashx
- Точка входа для удаленного RMS-сервиса или какого-либо http-клиента.

1.1. Администратор (admin.ashx)

При первом обращении какого-либо пользователя к сервису через **admin.ashx**, запрос перенаправляется методу **Login**, в ответ на который сервис возвращает страницу входа в систему. Пользователь-администратор сервиса вводит имя и пароль в соответствии с их значениями из файла **Rms.config**.

При правильном вводе имени и пароля, сервис авторизует пользователя и возвращает ему специальный токен безопасности. Этот токен существует до момента выхода пользователя из системы или до закрытия окна браузера. Токен – это специальная зашифрованная cookie, которая хранит имя пользователя. Она зашифрована ключом Web сервера и не запоминается браузером, а «путешествует» от браузера к сервису и обратно при каждом запросе.

Существуют ресурсы на сервисе, которые по тем или иным причинам не защищены. Проверка к доступу к ним не выполняется.

1.2. Web API (service.ashx)

Данная точка доступа представляет собой программный Web API механизм подключения к сервису. В отличие от **admin.ashx**, эта точка доступа не предоставляет графический GUI

интерфейс, т.е. не содержит Web-страниц. Через нее к сервису по http протоколу подключаются другие RMS-сервисы и/или различные клиенты.

Основной ресурс, запрашиваемый через **service.ashx** – это каналы сообщений. При подключении к каналу, удаленный клиент вызывает метод **Login** данной точки доступа и передает в качестве параметра виртуальный адрес канала и пароль. Для успешной аутентификации канал с таким именем должен быть зарегистрирован на данном сервисе, а переданный пароль должен совпадать с входным паролем, заданным в свойствах этого канала. В случае успешного подключения, сервис возвращает токен аутентификации. При каждом последующем запросе сервис проверяет наличие данного токена. Если он не передан, то сервис генерирует ошибку.

Для блокировки всех внешних запросов к **service.ashx**, сервис должен быть переведен администратором в **Offline** режим. Его работа будет продолжена в обычном режиме за исключением доступа к функционалу, предоставляемому Web API интерфейсом.

1.3. Заключение

Для обеспечения безопасного доступа к ресурсам сервиса используется ASP.NET Forms аутентификация. Ее преимущество состоит в том, что она мало затратная по ресурсам, не снижает быстродействие, не потребляет дополнительные мощности. Недостаток ее в том, что до момента авторизации, т.е. до момента получения токена аутентификации, имя и пароль передаются по сети в открытом виде. Для исключения такого вида угроз, применяется шифрование канала, т.е. протокол https.

Если сервис виден из сети Internet, то рекомендуется для всех каналов установить входящий пароль. Такой же пароль, только исходящий, необходимо будет установить у Remote-каналов на другом конце соединения. Входящий пароль не действует на локальный обмен сообщениями между двумя БД, т.к. в этом случае имя и пароль задаются в строке подключения к БД.

2. РЕКОМЕНДАЦИИ ПО ОСВОЕНИЮ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В документе используются следующие сокращения:

ПК – программный комплекс.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номер версии	Примечание	Дата	ФИО исполнителя
01	Начальная версия	02.03.2016	Пахомов Д.Г.