



**платформа аутентификации и управления
доступом**

Руководство разработчика

Часть 1

Общие сведения

Листов 30

Содержание

Перечень сокращений	3
Перечень терминов.....	4
1. Общие сведения	6
2. Описание сервисов	10
3. Общая схема интеграции	13
4. Описание типов организаций	15
5. Подключение ИС и управление ролевыми моделями	16
6. Проверка контрольной суммы запросов	17
6.1. Заголовки запроса	17
6.2. Заголовки ответа	17
6.3. Алгоритм расчета контрольной суммы	18
6.3.1. Запрос без тела с несколькими параметрами	18
6.3.2. Запрос с телом без параметров	24
6.4. Возможные ошибки.....	27
6.4.1. Список ошибок	27
6.4.2. Пример запроса с ответом в статусе 403	27
6.4.3. Пример запроса с ответом в статусе 401	28
6.5. Отключение проверки контрольной суммы	29
Лист регистрации изменений	30

Перечень сокращений

API	– application programming interface (программный интерфейс приложения)
ЕСИА	– единая система идентификации и аутентификации
ИНН	– идентификационный номер налогоплательщика
ИС	– информационная система
ОШС	– организационно-штатная структура
СНИЛС	– страховой номер индивидуального лицевого счёта
УЗ	– учётная запись

Перечень терминов

Авторизация	– предоставление субъекту доступа прав доступа, а также предоставление доступа в соответствии с установленными правилами управления доступом
Атрибут	– признак или свойство субъекта доступа или объекта доступа
Аутентификация	– действия по проверке подлинности субъекта доступа и (или) объекта доступа, а также по проверке принадлежности субъекту доступа и (или) объекту доступа предъявленного идентификатора доступа и аутентификационной информации
Двухфакторная аутентификация	– метод проверки подлинности субъекта доступа при помощи запроса аутентификационных данных двух разных типов
Динамическое поле	– признак или свойство учётной записи пользователя, профиля учётной записи пользователя или организации, добавляемый из внешних источников, в т. ч. может задаваться ИС путем взаимодействия с сервисом X-IDBox
Идентификатор	– признак субъекта доступа или объекта доступа в виде строки знаков (символов), который используется при идентификации и однозначно определяет (указывает) соотнесенную с ними идентификационную информацию
Идентификация	– действия по присвоению субъектам и объектам доступа идентификаторов и/или по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов
Интегрированная ИС	– ИС, подключенная к X-IDBox для использования её сервисов
Информационная система	– совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств
Контейнер ИС	– структурная единица ИС, предназначенная для хранения отдельных частей ролевой модели ИС и работы с ними
Объект доступа	– единица ИС (документ, поле, атрибут и т. п.), доступ к которой разграничивается политиками авторизации

Политика авторизации	– правило доступа, определяющее возможность выполнения действия или нескольких действий с ресурсом или несколькими ресурсами одного типа, при наличии у пользователя соответствующих назначенных ролей и выполнении заданного условия применимости политики авторизации
Приложение ИС	– структурная единица ИС, обеспечивающая возможность единого управления доступом в ИС, имеющую несколько приложений с идентичным или отличающимся набором функций, а также настройки способов аутентификации
Профиль учётной записи пользователя	– набор значений атрибутов учётной записи X-IDBox, однозначно ассоциирующий субъект доступа с организацией, в интересах (от имени) которой субъектом доступа выполняются операции, реализованные в X-IDBox и ИС, интегрированных с X-IDBox
Ресурс	– защищаемый объект ИС, который используется в политиках авторизации и относится к определенному типу ресурса
Роль	– предопределенная совокупность правил доступа к ресурсам (политик авторизации), устанавливающих допустимое взаимодействие между субъектами доступа и объектами доступа
Субъект доступа	– пользователь и/или ИС, действия которого по доступу к объектам доступа регламентируются политиками авторизации
Управление доступом	– ограничение и контроль доступа субъектов доступа к объектам доступа в информационной системе в соответствии с установленными правилами разграничения доступа
Учётная запись пользователя	– логический объект (совокупность данных пользователя), существующий в пределах X-IDBox и представляющий субъекта доступа в X-IDBox и ИС, интегрированных с X-IDBox

1. Общие сведения

X-IDBox представляет собой систему идентификации, аутентификации и разграничения доступа, имеющую встроенный механизм управления доступом.

X-IDBox обеспечивает процедуру единого входа во все ИС, интегрированные с X-IDBox, что позволяет выполнять переход между ИС без повторной аутентификации. Для каждой ИС возможна настройка способов аутентификации.

Подробное описание функций X-IDBox приведено в Руководстве пользователя.

Средствами внешних API X-IDBox обеспечивает выполнение следующих функциональных возможностей:

1) Управление УЗ пользователей (для всех ИС, интегрированных с X-IDBox, поддерживается единый каталог пользователей):

- загрузка списка пользователей из файла;
- загрузка изменения ролей профилей УЗ пользователей из файла;
- загрузка изменений личных данных пользователей из файла;
- загрузка обновления настроек динамических полей УЗ пользователей;
- загрузка источника динамических полей УЗ пользователей;
- получение данных об УЗ пользователя (по ИНН, по ИНН и СНИЛС, по СНИЛС, по идентификатору, по логину, по техническому наименованию ИС, по динамическим полям);
- получение списка профилей УЗ пользователя;
- получение настроек динамических полей УЗ пользователя;
- получение доступных источников динамических полей УЗ пользователей;
- удаление УЗ пользователя.

2) Управление профилями УЗ пользователей:

- загрузка профилей УЗ пользователей из файла;

- загрузка изменений сведений о профилях УЗ пользователей из файла;
- загрузка обновления настроек динамических полей профиля УЗ пользователя;
- загрузка источника динамических полей профилей УЗ пользователей;
- загрузка конфигурации источника динамических полей профиля УЗ пользователей из файла;
- назначение и снятие должностей с профилей УЗ пользователей;
- получение данных о профиле УЗ пользователя;
- получение информации о профиле УЗ пользователя;
- получение списка должностей профиля УЗ пользователя;
- получение списка ролей, назначенных профилю УЗ пользователя;
- получение сведений об ИС, в случае если у профиля УЗ пользователя есть хотя бы одна назначенная, действующая и активная роль в них;
- получение списка ресурсов, типов ресурсов и действий, доступных конкретному пользователю под конкретным профилем;
- получение списка профилей УЗ пользователей, для которых выполняется успешная авторизация для заданного ресурса и действия;
- получение настроек динамических полей профилей УЗ пользователей;
- получение доступных источников динамических полей профилей УЗ пользователей.

3) Управление ролями:

- загрузка ролевой модели ИС/контейнеров ИС из файла;
- загрузка изменений ролевой модели ИС/контейнеров ИС из файла;
- выгрузка перечня ролей ИС/контейнеров ИС в файл.

4) Управление ИС:

- регистрация ИС;
- обновление ИС;

- загрузка структуры ИС из файла;
- загрузка изменений структуры ИС из файла;
- выгрузка структуры ИС в ZIP-архив.

5) Управление приложениями ИС:

- загрузка приложений ИС;
- обновление приложений ИС.

6) Управление организациями:

- загрузка списка организаций и информации о них из файла;
- загрузка обновления настроек динамических полей организаций;
- загрузка источника динамических полей организаций;
- смена состояния (блокирование и разблокирование) организаций;
- определение ОШС организаций;
- изменение структуры подразделений и уровней подразделений в

ОШС организаций;

- изменение структуры должностей в ОШС организаций;
- получение данных об организации;
- получение списка организаций;
- получение списка подразделений организации;
- получение настроек динамических полей организаций.

7) Управление сессией пользователя:

- получения списка доступных способов аутентификации;
 - вход в систему по логину и паролю, по сертификату, с помощью
- доменной учётной записи (по протоколу Kerberos), через Госуслуги (ЕСИА);
- выход из системы;
 - запрос кода для выполнения двухфакторной аутентификации;
 - смена профиля УЗ текущего пользователя;
 - получение информации о текущем пользователе;

получение информации о профилях текущего пользователя.

8) Управление справочниками:

- загрузка справочника;
- изменение данных справочника;
- деактивация справочника.

2. Описание сервисов

В состав X-IDBox входят следующие сервисы:

1) Сервис идентификации – предоставляет по запросу идентификационные данные и атрибуты учётных записей пользователей, профилей учётных записей пользователей и организаций.

2) Сервис аутентификации – обеспечивает возможность аутентификации пользователей по логину и паролю, по сертификату, с помощью доменной учётной записи (по протоколу Kerberos), через Госуслуги (ЕСИА), а также возможность двухфакторной аутентификации. Сопоставляет предъявленные аутентификационные данные пользователя с данными, хранящимися в X-IDBox.

3) Сервис регистрации и изменения данных пользователей – предоставляет возможность загрузки списка пользователей и изменений данных пользователей, списка профилей УЗ пользователей и изменений данных профилей УЗ пользователей.

4) Сервис авторизации – проверяет наличие доступа у пользователя при его обращении к защищаемым объектам. Предоставляет информацию:

- о списке ИС, в которых у указанного профиля УЗ пользователя есть доступ;
- о списке доступных ресурсов и действий для конкретного профиля УЗ пользователя;
- о списке профилей УЗ пользователей, для которых выполняется успешная авторизация для заданного ресурса и действия;
- о списке ресурсных атрибутов участвующих в авторизации;
- о списке условий для успешного прохождения авторизации.

5) Сервис загрузки организаций – предоставляет возможность загрузки списка добавляемых или обновляемых организаций и изменения состояний организаций.

6) Сервис загрузки ОШС – предоставляет возможность загрузки ОШС организаций, вносимых изменений в данные подразделений и уровней подразделений в ОШС организации, вносимых изменений в данные подразделений в части доступных должностей.

7) Сервис загрузки назначений – предоставляет возможность загрузки информации о должностях и ролях и действиях с ними для конкретного профиля УЗ пользователя.

8) Сервис загрузки ролевых моделей – позволяет регистрировать и обновлять ИС, защищаемые объекты ИС (типы ресурсов, ресурсы, действия), условия применимости, политики авторизации, роли и их описания, связь ролевых групп, связи ролей с политиками авторизации и настройки ролей для обеспечения возможности последующего разграничения доступа пользователей к этим объектам.

9) Модуль отправки уведомлений информационным системам – обеспечивает отправку уведомлений информационным системам о произошедших событиях следующих типов:

- регистрация учётной записи пользователя;
- обновление данных учётной записи пользователя;
- регистрация профиля учётной записи пользователя;
- обновление данных учётной записи пользователя;
- изменение (назначение, обновление, снятие) ролей профиля учётной записи пользователя.

10) Сервис загрузки справочников – предоставляет возможность загрузки справочников, изменения данных справочников, деактивации справочников и загрузки конфигурации источника динамических полей профилей УЗ пользователей.

Описание работы с API указанных сервисов приведено в соответствующих документах:

- Руководство разработчика. Часть 2. Сервис идентификации;
- Руководство разработчика. Часть 3. Сервис загрузки ролевых моделей;

- Руководство разработчика. Часть 4. Сервис регистрации и изменения данных пользователей;
- Руководство разработчика. Часть 5. Сервис авторизации;
- Руководство разработчика. Часть 6. Сервис загрузки организаций;
- Руководство разработчика. Часть 7. Модуль отправки уведомлений информационным системам;
- Руководство разработчика. Часть 8. Сервис загрузки ОШС;
- Руководство разработчика. Часть 9. Сервис загрузки назначений;
- Руководство разработчика. Часть 10. Сервис аутентификации;
- Руководство разработчика. Часть 12. Сервис загрузки справочников.

Полный перечень сервисов X-IDBox приведен в Руководстве администратора.

Описание форматов файлов для загрузки через пользовательский интерфейс приведено в документе «Руководство разработчика. Часть 11. Форматы файлов для загрузки через пользовательский интерфейс». Подробное описание работы в пользовательском интерфейсе приведено в Руководстве пользователя.

Максимально допустимый размер файла для загрузки средствами внешних API и через пользовательский интерфейс зависит от конфигурации системы:

- в сервисе регистрации и изменения данных пользователей – 10 МБ;
- в сервисе загрузки организаций – 5 МБ;
- в сервисе загрузки ОШС – 2 МБ;
- в сервисе загрузки назначений – 10 МБ;
- в сервисе загрузки ролевых моделей – 8 МБ.

Допустимый размер файла для загрузки можно изменить с помощью настройки, приведённой в Руководстве администратора, в пределах указанных максимально допустимых значений.

3. Общая схема интеграции

Общая схема взаимодействия интегрированных ИС и X-IDBox приведена на рис. 1.

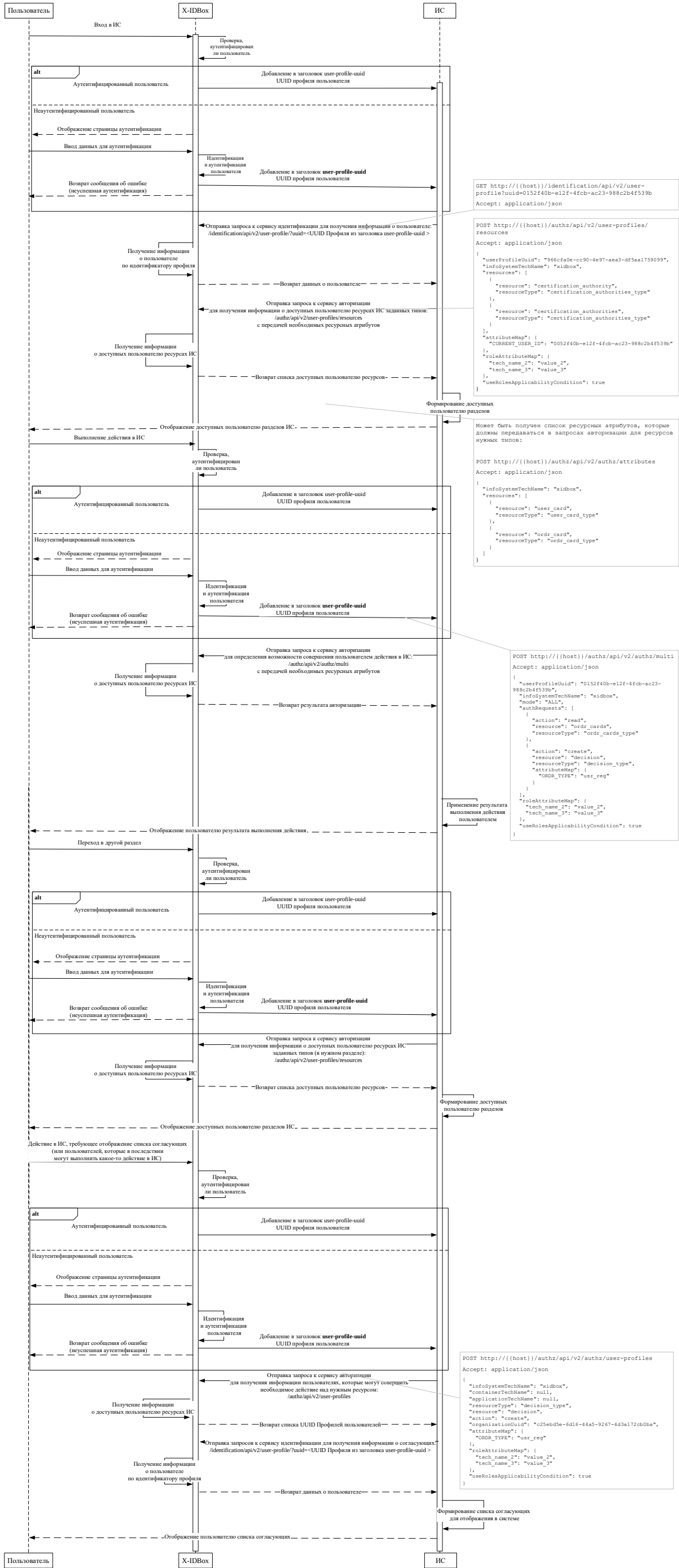


Рисунок 1 – Общая схема взаимодействия

4. Описание типов организаций

Типы организаций, которые поддерживаются в X-IDBox приведены в таблице 1.

Таблица 1 – Типы организаций

Тип организации		
Краткое наименование	Полное наименование	Техническое наименование
ЮЛ	Юридическое лицо	juristic
ОП	Обособленное подразделение (простое обособленное подразделение, филиал и представительство)	separate_juristic
КФХ	Крестьянское (фермерское) хозяйство	farming
ИП	Индивидуальный предприниматель	individual_entrepreneur
ФЛ	Физическое лицо	self_employed
НО	Не определён	not_defined

5. Подключение ИС и управление ролевыми моделями

Для подключения ИС к X-IDBox:

1) Ознакомьтесь с Руководством пользователя и Руководством разработчика (все части) X-IDBox.

2) Обеспечьте сетевую связанность между интегрированной ИС и X-IDBox:

– от X-IDBox до основного сервера приложений ИС или балансировщика нагрузки перед несколькими основными серверами приложений ИС;

– от серверов ИС до внешних сервисов X-IDBox.

3) Определите доменное имя ИС.

4) Предоставьте информацию для регистрации ИС. Необходимые данные для регистрации и подключения ИС приведены в Руководстве администратора.

5) Получите по результатам регистрации ИС секретный код ИС, используемый для формирования контрольной суммы при вызове сервисов X-IDBox.

6) Получите информацию о тестовом пользователе с ролью «Менеджер информационной системы» в X-IDBox для управления подключенной ИС средствами пользовательского интерфейса X-IDBox.

7) Подготовьте файл с описанием ролевой модели в соответствии с форматом X-IDBox. В соответствии с Руководством пользователя осуществите загрузку ролевой модели ИС. Управление ИС осуществляется в соответствии с Руководством пользователя.

Подробное описание подключения ИС приведено в Руководстве администратора.

6. Проверка контрольной суммы запросов

6.1. Заголовки запроса

Для доступа к API сервисов X-IDBox ИС необходимо рассчитывать контрольную сумму и передавать в запросах ряд заголовков, перечень которых приведён в таблице 2.

Таблица 2 – Заголовки запроса

Наименование заголовка	Обязательность	Описание
xidbox-request-auth-id	Да	Наименование заголовка запроса, в котором передается техническое наименование ИС, отправившей запрос
xidbox-request-application-id	Нет	Наименование заголовка запроса, в котором передается техническое наименование приложения, отправившего запрос
xidbox-request-timestamp	Да ¹⁾	Наименование заголовка запроса, в котором передается дата и время запроса
xidbox-request-checksum	Да ¹⁾	Наименование заголовка запроса, в котором передается контрольная сумма запроса
xidbox-request-algorithm	Да ¹⁾	Наименование заголовка запроса, в котором передается алгоритм расчёта контрольной суммы
xidbox-request-check-off	Нет ²⁾	Наименование заголовка – флага отключения сверки контрольной суммы
¹⁾ если в соответствии с настройками доступа ИС к сервису требуется передача и проверка контрольной суммы запроса ²⁾ данный заголовок используется только при включенном в X-IDBox режиме разработчика		

6.2. Заголовки ответа

Перечень заголовков ответов приведён в таблице 3.

Таблица 3 – Заголовки ответа

Наименование заголовка	Обязательность	Описание
xidbox-response-timestamp	Да ¹⁾	Наименование заголовка ответа, в котором передаются дата и время ответа

Наименование заголовка	Обязательность	Описание
xidbox-response-auth-id	Да ¹⁾	Наименование заголовка ответа, в котором передается техническое наименование ИС, отправившей запрос
xidbox-response-application-id	Нет ¹⁾	Наименование заголовка ответа, в котором передается техническое наименование приложения, отправившего запрос
xidbox-response-checksum	Да ¹⁾	Наименование заголовка ответа, в котором передается контрольная сумма ответа
xidbox-response-algorithm	Да ¹⁾	Наименование заголовка ответа, в котором передается алгоритм расчёта контрольной суммы
¹⁾ если в соответствии с настройками доступа ИС к сервису требуется передача контрольной суммы ответа		

6.3. Алгоритм расчета контрольной суммы

6.3.1. Запрос без тела с несколькими параметрами

Пример запроса без тела с несколькими параметрами:

```
GET http://{host}/identification/api/v1/user-profile/full?userProfileUuid=abe4abec-5f38-49a3-bfdd-a990e11e9435&dynamicFieldSourceTechName=FREE_IPA&organizationDynamicFieldSourceTechName=FREE_IPA
xidbox-request-auth-id: testis
xidbox-request-application-id: test_application
xidbox-request-timestamp: 2024-07-03T11:13:10.2515867Z
xidbox-request-algorithm: SHA256
xidbox-request-checksum:
aebb1552b5ee8bfe3cdfc4d49ec15b509c8d4e00e09bbe26f82a11de9fe4b701
Content-Type: application/json
Accept: application/json
```

Описание заголовков из запроса:

– **xidbox-request-auth-id: testis** – техническое наименование ИС, отправившей запрос (для примера – «testis»). Если не был передан заголовок

xidbox-request-application-id, то для ИС в X-IDBox должен быть настроен доступ к соответствующему сервису с указанием, что разрешено (чтение, запись), требуется ли передача и проверка контрольной суммы запросов, ответов, используемый алгоритм хеширования (поддерживаемые алгоритмы: MD2, MD5, SHA1, SHA256, SHA384, SHA512);

– **xidbox-request-application-id: test_application** – необязательный заголовок, содержит техническое наименование приложения ИС, отправившего запрос (для примера – «test_application»). Для приложения в X-IDBox должен быть настроен доступ к соответствующему сервису с указанием, что разрешено (чтение, запись), требуется ли передача и проверка контрольной суммы запросов, ответов, используемый алгоритм хеширования (поддерживаемые алгоритмы: MD2, MD5, SHA1, SHA256, SHA384, SHA512), либо приложение должно быть настроено для использования настроек доступа ИС;

– **xidbox-request-timestamp: 2024-07-03T11:13:10.2515867Z** – дата и время запроса. Обязательно должны быть в формате «Unix timestamp» или «ISO-8601 with TimeZone (ISO_OFFSET_DATE_TIME, ISO_INSTANT)»;

– **xidbox-request-algorithm: SHA256** – алгоритм, по которому сгенерирована контрольная сумма запроса. Поддерживаемые алгоритмы: MD2, MD5, SHA1, SHA256, SHA384, SHA512;

– **xidbox-request-checksum:**
aebb1552b5ee8bfe3cdfc4d49ec15b509c8d4e00e09bbe26f82a11de9fe4b701 – заголовок с контрольной суммой. Контрольная сумма запроса – это хеш строки: body + url + query + timestamp + authId + applicationId (если указан) + secret, вычисленный по алгоритму, указанному в заголовке «xidbox-request-algorithm».

Описание параметров из примера запроса приведено в таблице 4.

Таблица 4 – Параметры примера запроса

Наименование параметра	Значение	Описание
body	–	Тело запроса отсутствует
url	/identification/api/v1/user-profile/full	Не включает в себя host и параметры. Знак «/» в конце учитывается, если есть

Наименование параметра	Значение	Описание
query	FREE_IPA + FREE_IPA + abe4abec-5f38-49a3-bfdd-a990e11e9435	Параметры запроса, используются только значения, отсортированные по ключу (сортировка регистронезависимая)
timestamp	2024-07-03T11:13:10.2515867Z	Значение заголовка «xidbox-request-timestamp»
authId	testis	Значение заголовка «xidbox-request-auth-id»
applicationId	test_application	Значение заголовка «xidbox-request-application-id» (если указан)
secret	75ebe147-cc8c-4a30-9aaf-35141e0962b2	Секретный код ИС testis. Если приложение (значение заголовка «xidbox-request-application-id») не указано, или приложение настроено для использования настроек доступа ИС, то используется секретный код ИС testis. Иначе используется секретный код приложения test_application

Пример расчёта и вывода контрольной суммы:

```
echo -n '/identification/api/v1/user-
profile/fullFREE_IPAFREE_IPAabe4abec-5f38-49a3-bfdd-
a990e11e94352024-07-
03T11:13:10.2515867Ztestistest_application75ebe147-
cc8c-4a30-9aaf-35141e0962b2' | sha256sum
```

```
aebb1552b5ee8bfe3cdfc4d49ec15b509c8d4e00e09bbe26f82a1
1de9fe4b701
```

Если контрольная сумма корректна, сервис возвращает ответ на запрос;
если нет – возвращается сообщение об ошибке.

Пример положительного ответа с добавленными заголовками:

```
HTTP/1.1 200
xidbox-response-timestamp: 2024-07-
03T11:57:58.5177638Z
xidbox-response-auth-id: testis
xidbox-response-application-id: test_application
xidbox-response-checksum:
1c40415917e4d584b2fc4ac0368286f81842f3dd49668156dcdc8
03e6b555d72
xidbox-response-algorithm: SHA256
Content-Type: application/json
```

```
Content-Length: 2346
Date: Wed, 03 Jul 2024 11:57:58 GMT
Keep-Alive: timeout=60
Connection: keep-alive

{
  "uuid": "abe4abec-5f38-49a3-bfdd-a990e11e9435",
  "isBlocked": false,
  "state": "ACTIVE",
  "workEmail": "liza@localhost.ru",
  "workEmailVerified": "2024-01-23T06:51:09.870305Z",
  "registrationDate": "2024-01-23T06:50:35.456343Z",
  "user": {
    "uuid": "14dad2b2-e7ac-4bb4-ab01-616a9d3c2128",
    "firstName": "Елизавета",
    "lastName": "Беляева",
    "middleName": "Артёмовна",
    "inn": null,
    "snils": null,
    "birthday": "1996-10-25",
    "login": "liza",
    "email": "liza@localhost.ru",
    "passwordChanged": "2024-01-23T06:51:09.860989Z",
    "emailVerified": "2024-01-23T06:51:09.870305Z",
    "isBlocked": false,
    "state": "ACTIVE",
    "privacyPolicyAccepted": "2024-01-23T06:45:19.724706Z"
  },
  "organization": {
    "uuid": "087a7cae-8cd3-44d5-896b-e86102164bba",
    "fullName": "АО Авоир дремучий",
    "shortName": "АО Авоир дремучий",
    "typeTechName": "juristic",
    "typeLabel": "Юридическое лицо",
    "inn": "2252455070",
    "kpp": "037271508",
    "ogrn": "1463527365443",
    "isBlocked": false,
    "state": "ACTIVE",
```

```
"address": "Московская обл., г. Москва, ул.  
Московская д.4, оф.2",  
"registrationDate": null,  
"createDate": "2023-01-28T09:20:36.355757Z",  
"dynamicFields": null  
},  
"dynamicFields": {  
  "sourceUuid": "5c84b6a9-6a28-483f-a40f-  
ea8b6159fcf3",  
  "sourceTechName": "FREE_IPA",  
  "sourceLabel": "FREE_IPA",  
  "dynamicFields": [  
    {  
      "uuid": "b7e5c345-6981-4a7e-aed0-  
194360d7b661",  
      "label": "Страна",  
      "techName": "city",  
      "content": {  
        "value": "Вьетнам",  
        "isDeleted": false  
      }  
    },  
    {  
      "uuid": "ead47367-9a18-41be-9711-  
60e48de70a64",  
      "label": "Уникальный идентификатор профиля  
LDAP",  
      "techName": "ipaUniqueProfileID",  
      "content": {  
        "value": null,  
        "isDeleted": true  
      }  
    },  
    {  
      "uuid": "ebfe666a-4e71-49b2-89e3-  
37827bc9109f",  
      "label": "Город",  
      "techName": "l",  
      "content": {  
        "value": "Ханой",
```

```
        "isDeleted": false
      }
    },
    {
      "uuid": "9ffcf3a38-96e0-4c20-8c7d-
35eb328f59ff",
      "label": "Номер телефона",
      "techName": "mobile",
      "content": {
        "value": null,
        "isDeleted": true
      }
    }
  ]
},
"organizationDynamicFields": {
  "sourceUuid": "3557063c-3836-4f5a-8697-
9ed9574e5782",
  "sourceTechName": "FREE_IPA",
  "sourceLabel": "FREE_IPA",
  "dynamicFields": [
    {
      "uuid": "cb4c2043-fc45-4205-8d17-
83e696d4cbbd",
      "label": "Уникальный идентификатор LDAP",
      "techName": "entryUUID1",
      "content": {
        "value": "CN=Авоир Дремучий
АД, CN=Organizations, DC=xidbox, DC=dcs, DC=infosec, DC=ru
",
        "isDeleted": false
      }
    }
  ]
},
"positions": []
}
```

6.3.2. Запрос с телом без параметров

Пример запроса с телом без параметров:

```
POST
http://{{host}}/identification/api/v1/information-
system/all
xidbox-request-auth-id: testis
xidbox-request-timestamp: 2024-07-
03T11:13:10.2515867Z
xidbox-request-algorithm: SHA256
xidbox-request-checksum:
605b599f85f89cc0da1b27b42181315330e64a233ed7aec71b093
44973dc2b27
Content-Type: application/json
Accept: application/json

{
  "limit": 10,
  "name": "NKG DYXZJQ",
  "techName": "_nKWgDY",
  "shortName": "autotest"
}
```

Описание заголовков из запроса:

- **xidbox-request-auth-id: testis** – идентификатор ИС, отправившей запрос. (для примера – «testis»). Для ИС в X-IDBox должен быть настроен доступ к соответствующему сервису с указанием, что разрешено (чтение, запись), требуется ли передача и проверка контрольной суммы запросов, ответов, используемый алгоритм хеширования (поддерживаемые алгоритмы: MD2, MD5, SHA1, SHA256, SHA384, SHA512);
- **xidbox-request-timestamp: 2024-07-03T11:13:10.2515867Z** – дата и время запроса. Обязательно должны быть в формате «Unix timestamp» или «ISO-8601 with TimeZone (ISO_OFFSET_DATE_TIME, ISO_INSTANT)»;

– **xidbox-request-algorithm: SHA256** – алгоритм, по которому сгенерирована контрольная сумма запроса. Поддерживаемые алгоритмы: MD2, MD5, SHA1, SHA256, SHA384, SHA512;

– **xidbox-request-checksum:**

605b599f85f89cc0da1b27b42181315330e64a233ed7aec71b09344973dc2b27 –

заголовок с контрольной суммой. Контрольная сумма запроса – это хеш строки: body + url + query + timestamp + authId + secret, вычисленный по алгоритму, указанному в заголовке «xidbox-request-algorithm».

Описание параметров из примера запроса приведено в таблице 5.

Таблица 5 – Параметры примера запроса

Наименование параметра	Значение	Описание
body	{ "limit": 10, "name": "NKGWGDYXZJQ", "techName": "_nKWgDY", "shortName": "autotest" }	Тело запроса. Если запрос проводит загрузку данных в виде файла, телом запроса является содержимое загружаемого файла
url	/identification/api/v1/information-system/all	Не включает в себя host и параметры Знак «/» в конце учитывается, если есть
query	–	Параметры у запроса отсутствуют
timestamp	2024-07-03T11:13:10.2515867Z	Значение заголовка «xidbox-request-timestamp»
authId	testis	Значение заголовка «xidbox-request-auth-id»
secret	75ebe147-cc8c-4a30-9aaf-35141e0962b2	Секретный код ИС testis

Пример расчёта и вывода контрольной суммы:

```
echo -n '{
  "limit": 10,
  "name": "NKGWGDYXZJQ",
  "techName": "_nKWgDY",
  "shortName": "autotest"
}/identification/api/v1/information-system/all2024-
07-03T11:13:10.2515867Ztestis75ebe147-cc8c-4a30-9aaf-
35141e0962b2' | sha256sum
```

605b599f85f89cc0da1b27b42181315330e64a233ed7aec71b093
44973dc2b27

Пример положительного ответа с добавленными заголовками:

```
HTTP/1.1 200
xidbox-response-timestamp: 2024-07-
03T12:09:17.9413322Z
xidbox-response-auth-id: testis
xidbox-response-checksum:
43e446ae4f7e62ebb00b2d6a8299e473f34fa0c4e3851a9fb3944
f78053bc893
xidbox-response-algorithm: SHA256
Content-Type: application/json
Content-Length: 327
Date: Wed, 03 Jul 2024 12:09:17 GMT
Keep-Alive: timeout=60
Connection: keep-alive
```

```
[
  {
    "uuid": "e0af68a9-7e62-402a-9342-75cf3e38be56",
    "techName": "AUTOTEST_SYSTEM_NKWGDYXZJQ",
    "name": "AutotestSystemNkwgdyxzjq",
    "shortName": "AUTOTEST-SYSTEM-NKWGDYXZJQ"
  },
  {
    "uuid": "8fae4d62-1227-47d2-ad8e-cb776a328056",
    "techName": "autotest_system_nKWgDYXZJQ",
    "name": "AutotestSystemNkwgdyxzjq",
    "shortName": "autotest-system-nKWgDYXZJQ"
  }
]
```

6.4. Возможные ошибки

6.4.1. Список ошибок

Описание возможных ошибок приведено в таблице 6.

Таблица 6 – Возможные ошибки

Статус	Ошибка	Причина
401	UNAUTHORIZED	Отсутствие одного из обязательных заголовков
401	UNAUTHORIZED	У ИС нет доступа к сервису
401	UNAUTHORIZED	Указан некорректный или неподдерживаемый алгоритм генерации контрольной суммы в заголовке «xidbox-request-algorithm» или настройке алгоритма формирования контрольной суммы ответа в настройках ИС в X-IDBox
401	UNAUTHORIZED	Некорректная контрольная сумма
401	UNAUTHORIZED	Приложение, указанное в заголовке, не существует
403	FORBIDDEN	Неверный формат даты в заголовке «xidbox-request-timestamp». Превышение максимальной разницы с временем сервера
403	FORBIDDEN	Отсутствие у ИС доступа к методам GET или PUT, POST, DELETE в соответствии с настройками доступа к сервису

6.4.2. Пример запроса с ответом в статусе 403

Причина ошибки – некорректный формат значения заголовка «xidbox-request-timestamp».

```
GET
http://{{host}}/identification/api/v1/user?snils=1008
7511016&inn=836767631381
xidbox-request-auth-id: testis
xidbox-request-timestamp: 2024-07-04T16:00:50
xidbox-request-algorithm: SHA256
```

```
xidbox-request-checksum:
54fcac9faf374436b374db7b3badca7bdbbb68cca5aa6f411eada
cb0babd3dc2
Content-Type: application/json
Accept: application/json
```

```
### response example
HTTP/1.1 403
Content-Type: application/json
Transfer-Encoding: chunked
Date: Thu, 04 Jul 2024 16:00:51 GMT
Keep-Alive: timeout=60
Connection: keep-alive
```

```
{
  "timestamp": "2024-07-04T16:00:51.491+00:00",
  "status": 403,
  "error": "Forbidden",
  "path": "/identification/api/v1/user"
}
```

6.4.3. Пример запроса с ответом в статусе 401

Причина ошибки – неверная контрольная сумма запроса.

```
GET
http://{{host}}/identification/api/v1/user?snils=1008
7511016&inn=836767631381
xidbox-request-auth-id: testis
xidbox-request-timestamp: 2024-07-
04T16:11:55.2515867Z
xidbox-request-algorithm: SHA256
xidbox-request-checksum:
54fcac9faf374436b374db7b3badca7bdbbb68cca5aa6f411eada
cb0babd3dc2
Content-Type: application/json
Accept: application/json
```

```
### response example
HTTP/1.1 401
```

```
Content-Type: application/json
Transfer-Encoding: chunked
Date: Thu, 04 Jul 2024 16:12:31 GMT
Keep-Alive: timeout=60
Connection: keep-alive

{
  "timestamp": "2024-07-04T16:12:31.755+00:00",
  "status": 401,
  "error": "Unauthorized",
  "path": "/identification/api/v1/user"
}
```

6.5. Отключение проверки контрольной суммы

Отключение проверки контрольной суммы в конкретном запросе возможно при включенном режиме разработчика в X-IDBox.

Для отключения проверки контрольной суммы в запросах должен быть передан дополнительный заголовок «xidbox-request-check-off» с любым значением или без него. При этом необходимо передавать все обязательные заголовки запроса (п. 6.1), доступ к сервису у ИС должен быть.

Лист регистрации изменений

Версия	Изменения
1.0.0	Начальная версия
1.0.1	—
1.0.2	—
1.0.3	—
1.0.4	В описание типов организаций добавлен тип «not_defined»
1.1.0	В описании общих сведений дополнены функциональные возможности X-IDBox, обеспечиваемые средствами внешних API
	В описание проверки контрольной суммы запросов добавлены необязательные заголовки запроса «xidbox-request-application-id» и ответа «xidbox-response-application-id»
	В описании сервисов добавлен сервис загрузки справочников
	Обновлены примеры запросов на общей схеме интеграции
	В описании сервисов добавлено примечание об ограничении размера файла для загрузки