



**Акционерное общество «Национальная платежная корпорация
Национального Банка Республики Казахстан»**

**Утверждаю
И.о Председателя
Правления АО «НПК»**

_____ Самаева Ж. Т.
« » _____ 2024 г.

**Техническая документация сервиса сопоставления фотоизображений
информационной системы «Центр обмена идентификационными данными»**

2024 г.

Должность, подразделение разработчика	ФИО	Подпись	Дата
Главный системный аналитик операционного сопровождения управления ЦОИД	Р. Халиков		

ЛИСТ СОГЛАСОВАНИЯ

№ п/п	Должность	ФИО	Подпись	Дата
1.	Начальник управления информационной безопасности	Т. Муканов		
2.	Начальник управления ЦОИД	А. Ермаханова		

№ п/ п	Дата редакции документа	Номер редакции документа	Изменения
1		1	
2		1.1	В разделе 6, подразделов 6.1 и 6.2, в ответ добавлены фотография в формате base64, реквизиты заказчика биометрической идентификации, а также дата и время обработки запроса.
3		1.2	В разделе «Термины и понятия, используемые в документе» добавлено упоминание об алгоритме ЭЦП ГОСТ 34.10-2015 РК. В разделе 6, подраздел 6.6 исключен метод получения расшифровки файлов. За место него реализован метод получения JSON массива с расшифровкой.
4		1.3	В разделе «Термины и понятия, используемые в документе» добавлено упоминание об удостоверяющем центре. Изменено приложение 5 касательно формирования ЭЦП JWS. Добавлено приложение 6 касательно проверки ЭЦП JWS.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	6
1. Термины и понятия, используемые в документе	7
2. Цель и область применения ЦОИД	8
3. Участники ЦОИД и их функции	8
4. Процесс сервиса сопоставления фотоизображений ЦОИД	10
5. Общая архитектура ЦОИД	12
6. Описание методов системы ЦОИД.....	13
<i>Приложение 1</i>	23
Требование к изображениям	23
Заголовки HTTP запроса	25
Заголовки ответа.....	26
<i>Приложение 4</i>	27
Коды статусов ответа.....	27
<i>Приложение 5</i>	30
Формирование ЭЦП JWS	30
<i>Приложение 6</i>	32
Проверка ЭЦП JWS.....	32

ВВЕДЕНИЕ

Данный документ был разработан в целях описания механизма удаленной идентификации клиентов финансовых организаций, заинтересованных в получении финансовых услуг дистанционным способом, в рамках реализации мероприятий государственной программы «Цифровой Казахстан» (Постановление Правительства Республики Казахстан от 12 декабря 2017 года № 827).

В соответствии с пунктом 1 статьи 5 Закона Республики Казахстан от 28 августа 2009 года № 191-IV «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» и соответствующими подзаконными актами, регулирующими оказание финансовых услуг, субъектам финансового мониторинга предоставляются услуги сервиса сопоставления фотоизображений информационной системы «Центр обмена идентификационными данными» (далее – ЦОИД) для надлежащей проверки клиентов при установлении деловых отношений дистанционным способом.

Надлежащая проверка клиента на стороне ЦОИД обеспечивается в соответствии с Требованиями к надлежащей проверке клиентов субъектами финансового мониторинга (*постановление Правления Национального Банка Республики Казахстан от 29 июня 2018 года № 140*), с применением средств биометрической идентификации и сверки биометрических данных клиента с данными из Государственных баз данных «Физические лица» (далее – ГБД ФЛ).

1. Термины и понятия, используемые в документе

В настоящем документе используются понятия, предусмотренные Законами Республики Казахстан «О платежах и платежных системах» от 26 июля 2016 года № 11-VI ЗРК, «О национальных реестрах идентификационных номеров» от 12 января 2007 года № 223-III ЗРК, «Об электронном документе и электронной цифровой подписи» от 7 января 2003 года № 370-II, «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» от 28 августа 2009 года № 191-IV ЗРК, «О дактилоскопической и геномной регистрации» от 30 декабря 2016 года № 40-VI ЗРК, «О персональных данных и их защите» от 21 мая 2013 года N 94-V, Правилами оказания банками и организациями, осуществляющими отдельные виды банковских операций, электронных банковских услуг, утвержденные постановлением Правления Национального Банка Республики Казахстан от 31 августа 2016 года № 212, а также следующие понятия:

АО «НПК» – Акционерное Общество «Национальная платежная корпорация Национального Банка Республики Казахстан»;

Клиент – физическое лицо, в отношении которого производится идентификация;

Участник – банк второго уровня, организация, осуществляющая отдельные виды банковских операций и небанковская организация;

Небанковская организация – юридическое лицо, не имеющее лицензию на проведение банковских операций;

ЭЦП – Электронно-цифровая подпись по алгоритму ГОСТ 34.310-2004 РК и/или ГОСТ 34.10-2015 РК;

УЦ – Удостоверяющий Центр структурное подразделение АО «НПК», уполномоченное в установленном порядке на выпуск и управление сертификатами электронной цифровой подписи (ЭЦП). Удостоверяющий центр осуществляет подтверждение подлинности ключей подписи и обеспечивает юридическую значимость электронных документов, создаваемых и подписываемых с использованием этих сертификатов.

ПАК «Шлюз НБРК» – Программно-аппаратный комплекс «Шлюз НБРК», предназначенный для интеграции информационных систем Национального Банка с базовыми компонентами «электронного правительства» и информационными системами Министерства юстиции РК;

КДП – Сервис контроля доступа к персональным данным;

API (Application Programming Interface) – программный интерфейс приложения, интерфейс прикладного программирования;

REST (Representational State Transfer) – архитектурный стиль взаимодействия компонентов распределённого приложения в сети;

JSON (JavaScript Object Notation) – текстовый формат обмена данными, основанный на JavaScript;

Оператор – Оператор ЦОИД, которым выступает НПК;

Идентификация – совокупность мероприятий по установлению определенных законодательством Республики Казахстан сведений о клиенте и подтверждению

достоверности этих сведений. В рамках настоящего документа идентификация осуществляется путем присвоения или определения соответствия предъявленного для получения доступа в систему и/или к ресурсу системы идентификатора перечню идентификаторов, имеющих в системе;

Поставщик биометрического решения – компания - производитель биометрических процессоров, поставляющая их под своей маркой;

Видеоинтервью – проведение сеанса видеоконференции с менеджером Участника или в автоматизированном режиме с применением специализированного приложения, реализующего технологию выявления манипуляций и/или подлога фактического участия, интервьюируемого в процессе дистанционной идентификации.

2. Цель и область применения ЦОИД

Основная цель сервиса сопоставления фотоизображений ЦОИД – предоставление безопасного и эффективного механизма удаленной идентификации, способного обеспечить онлайн идентификацию Клиентов без его физического присутствия.

Область применения ЦОИД включает:

- удаленную идентификацию «новых» клиентов, ранее не имевших деловых отношений с финансовыми или платежными организациями;
- получение верифицированных данных клиентов по запросу из ГБД ФЛ.

При этом решение по предоставлению услуги и управлению рисками при предоставлении услуг дистанционным способом принимаются Участниками самостоятельно.

Указанный сервис также может быть использован при off-line обслуживании клиентов (личное посещение Участника) путем передачи менеджером Участника ИИН и фото клиента в ЦОИД.

3. Участники ЦОИД и их функции

Участник	Описание
Оператор (АО «НПК»)	Операционный центр, обеспечивающий взаимодействие с Участниками по обмену данными клиентов из доступных источников для проведения процедуры их идентификации. Оператор имеет доступ к ГБД ФЛ, в которой содержатся верифицированные данные клиентов, необходимые для выполнения требований по надлежащей проверке Клиентов в соответствии с ПОД/ФТ, а также фотоизображение Клиентов из документов, удостоверяющих личность. Оператор посредством сервиса сопоставления фотоизображений ЦОИД сличает фотоизображение клиента, полученное из сеанса видеоконференции или с применением специализированного программного обеспечения, реализующего технологию выявления манипуляций и/или

	подлога фактического участия в процессе дистанционной идентификации, с фотоизображением Клиента полученного из ГБД ФЛ. Результаты степени соответствия по биометрическим показателям фотоизображений и, в случае успешной процедуры сверки - идентификационные данные Клиента передаются Участнику. Результаты степени соответствия и информация по запросам хранятся в базе данных ЦОИД.
Министерство юстиции Республики Казахстан (АО «Национальные информационные технологии» (далее – АО «НИТ»))	Владелец ГБД ФЛ. Оператор, в лице АО «НИТ» обеспечивает по запросу предоставление верифицированных данных клиентов, необходимых для выполнения требований ПОД/ФТ и фотоизображения Клиента из документов, удостоверяющих личность, содержащихся в ГБД ФЛ.
Национальный Банк Республики Казахстан	Национальный Банк Республики Казахстан предоставляет доступ Оператору к площадке Программно-аппаратного комплекса «Шлюз НБРК» для получения данных из ГБД «ФЛ» в режиме 24/7/365. В случае возникновения внештатных ситуаций, влияющих на работу ПАК «Шлюз НБРК», НБРК должен своевременно оповестить Оператора.
Комитет информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Казахстана	Владелец ИС КДП. Оператор, в лице АО «НИТ» обеспечивает по запросу предоставление доступа к персональным данным после получения соответствующего согласия со стороны гражданина.
Участник	Юридическое лицо, предоставляющее финансовые услуги Клиенту (открытие счета, выдача кредита и т.д.). При этом в целях дистанционной идентификации клиента, Участник направляет в ЦОИД фото, полученное из сеанса видеоконференции или в автоматизированном режиме с применением специализированного приложения для осуществления процедуры сверки.
Клиент	Клиентом может выступать физическое лицо, являющееся резидентом Республики Казахстан. Клиент взаимодействует с Участником для получения финансовых/платежных услуг дистанционным способом.

4. Процесс сервиса сопоставления фотоизображений ЦОИД

На рисунке ниже представлен основной сценарий, который должен выполняться в рамках сервиса сопоставления фотоизображений ЦОИД (рис.1).

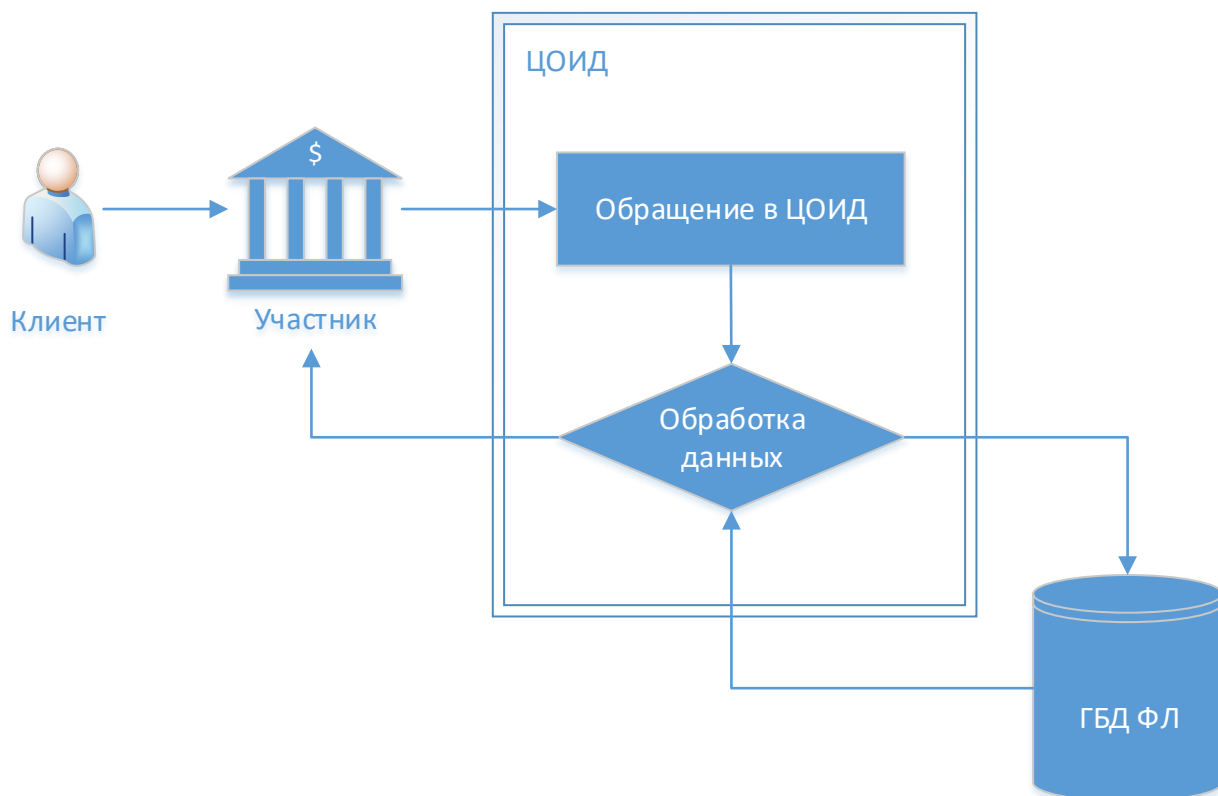


Рис.1. Основной сценарий ЦОИД

Для отправки запроса на сопоставление фотоизображения Клиента Участник должен:

- 1) получить согласие Клиента на сбор, обработку и передачу его персональных данных, в том числе третьими лицами;
- 2) убедиться в том, что Клиентом не используются фотоизображения, видеозаписи, маски и иные средства/технологии для подмены личности Клиента.

Сервис сопоставления фотоизображения Клиента принимает следующие виды и параметры запросов:

- 1) запрос на получение результатов степени соответствия фотоизображения Клиента, который содержит:
 - ИИН Клиента;
 - фотоизображение Клиента, полученное от Участника с применением специализированного программного обеспечения, реализующего технологию выявления подмены личности Клиента в процессе дистанционной идентификации, удовлетворяющее требованиям, приведенным в Приложении 1.

2) запрос на получение персональных данных Клиента, содержащий подписанное электронной цифровой подписью Участника подтверждение наличия согласия Клиента на сбор, обработку и передачу его персональных данных третьим лицам.

Сервис ЦОИД осуществляет обработку запроса Участника, удовлетворяющего форматам обмена запросами, в следующем порядке:

1) направляет в доступные источники запрос на получение фотоизображения Клиента;

2) направляет фотоизображения Клиента, полученные от Участника и доступных источников биометрическому решению сопоставления фотоизображений для сопоставления;

3) перенаправляет Участнику ответ биометрического решения сопоставления фотоизображений о степени соответствия обработанных фотоизображений;

4) в случае если степень соответствия фотоизображений выше 85%, сервис сопоставления фотоизображений, по запросу Участника, направляет в доступные источники запрос на получение персональных данных Клиента.

5) Полученные персональные данные перенаправляются Участнику;

Если степень соответствия фотоизображений ниже 85% сервис сопоставления фотоизображений направляет Участнику результат степени соответствия. При степени соответствия фотоизображений ниже 85%, сервис сопоставления фотоизображений не предоставляет персональные данные Клиента Участнику.

При проценте верификации фотоизображения клиента ниже 85% Участник самостоятельно принимает решение о возможности идентификации по предоставленному проценту степени соответствия и о дальнейшем установлении деловых отношений клиентом.

Фотоизображение, полученное из видеоинтервью Участника с Клиентом, подлежит хранению в базе данных ЦОИД.



Схема 1. Бизнес-процесс ЦОИД идентификации по фотоизображению

Изображения, не соответствующие критериям, указанным в приложении 1, будут отклонены.

Для получения данных из ГБД ФЛ ЦОИД взаимодействует с ПАК Шлюзом НБ РК.

ЦОИД направляет 3 запроса в ГБД ФЛ:

- на получение токена доступа к персональным данным по ИИН;
- на получение фотоизображения клиента по ИИН;
- на получение персональных данных по ИИН при представлении

Участником подтверждения о получении согласия клиента на обработку и передачу его (ее) персональных данных третьим лицам и верификации от 85% и выше.

ЦОИД определяет степень соответствия по биометрическим показателям фотоизображений. Результаты степени соответствия клиента, полученные ЦОИД принимаются с совпадением 85 % и выше.

При проценте сличения менее 85% Участником самостоятельно принимается решение о включении клиента в базу «Мошенники», о чем Участник информирует Оператора. Участник, при необходимости, передает информацию в правоохранительные органы. При успешном проведении верификации (85% и выше) ЦОИД направляет Участнику информацию о результатах степени соответствия.

5. Общая архитектура ЦОИД

Система ЦОИД – платформа по определению степени соответствия (верификации) полученного фотоизображения из видеосюбъекта с эталонным

фотоизображениям, а также получением персональных данных из ГБД ФЛ, система предоставляет REST API для взаимодействия с Участниками.

Обмен данными Участника с ЦОИД будет осуществляться в электронном формате с использованием защищенного канала связи.

На рисунке ниже представлена архитектура ЦОИД.

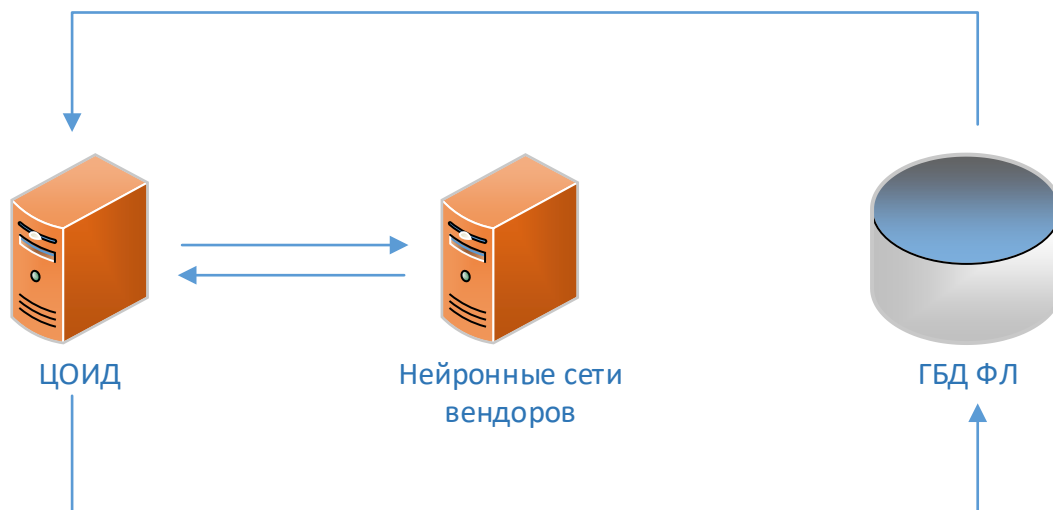


Рис. 2. Архитектура ЦОИД

ЦОИД – программное обеспечение, предоставляемое Оператором и направленное на установление взаимосвязей между программными компонентами ЦОИД и Участников. ЦОИД включает в себя:

- взаимодействие с ИС КДП для получения токена доступа к персональным данным по ИИН;
- взаимодействие с ГБД ФЛ для направления запросов и получения ответов из ГБД ФЛ. Следует учесть, что взаимодействие будет проходить в 2 этапа, первый запрос ЦОИД будет запрашивать фотографию Клиента из базы данных, второй запрос направлен на получение персональных данных Клиента из ГБД ФЛ;
- взаимодействие с нейронными сетями вендоров для получения степени соответствия полученного фотоизображения из видеоинтервью с эталонными фотоизображениями, полученными из ГБД ФЛ.

6. Описание методов системы ЦОИД

6.1. Запрос на проведение процесса верификации

Request:

POST <https://onlinetest.kisc.kz/identity/1.1.0/verify?iin=123456789012&vendor=1>

x-idempotency-key: CD0305201705

Content-Type: image/png

{

<бинарные данные фото>
}

Описание заголовков запроса см. в приложении 2.

Параметр запроса:

Поле	Тип	Описание
iin	string	ИИН клиента
vendor	int	Код поставщика алгоритма

Описание полей тела запроса:

Поле	Тип	Описание
	binary	Бинарные данные фото

Response:

HTTP/1.1 200 OK

x-jws-signature: WGJlkaHzz5VAKdukFIOl

Content-Type: application/json

```
{
  "iin": "123456789012",
  "vendor": "VisionLabs",
  "result": 0.9959589839,
  "x_idempotency_key": "CD0305201705",
  "photo": "/9j/4AQWESDQWERSSDSDSDSDSDSDSDSD",
  "requisites": {
    "name": "ТОО \"Наименование организации\"",
    "bin": "123456789012"
  },
  "requestDate": "2024-10-17T11:49:01.337+00:00"
}
```

Описание заголовков запроса см. в приложении 2.

Участник должен сохранить json документ и x-jws-signature подпись из заголовка, а также произвести проверку подписи.

Описание полей тела ответа:

Поле	Тип	Описание
iin	string	ИИН клиента
vendor	string	Название поставщика алгоритма
result	float	Степень схожести

x_idempotency_key		string	Ключ идемпотентности
photo		string	Фото в формате Base64
requisites		object	Реквизиты
	name	string	Наименование организации
	bin	string	БИН организации
requestDate		DateTime	Дата и время UTC+5

6.2. Запрос на получение степени соответствия

Request:

GET https://onlinetest.kisc.kz/identity/1.1.0/verify

x-idempotency-key: CD0305201705

Описание заголовков запроса см. в приложении 2.

Response:

HTTP/1.1 200 OK

Content-Type: application/json

```
{
  "iin": "123456789012",
  "vendor": "VisionLabs",
  "result": 0.9959589839,
  "x_idempotency_key": "CD0305201705",
  "photo": "",
  "requisites": {
    "name": "ТОО \"Наименование организации\"",
    "bin": "123456789012"
  },
  "requestDate": "2024-10-17T11:49:01.337+00:00"
}
```

Описание заголовков запроса см. в приложении 2.

Описание полей тела ответа:

Поле	Тип	Описание
iin	string	ИИН клиента
vendor	string	Название поставщика алгоритма
result	float	Степень схожести
x_idempotency_key	string	Ключ идемпотентности

photo	string	Фото отсутствует
requisites	object	Реквизиты
	name	Наименование организации
	bin	БИН организации
requestDate	DateTime	Дата и время UTC+5

6.3. Запрос на получение персональных данных клиента из ГБД ФЛ

Request:

POST https://onlinetest.kisc.kz/identity/1.1.0/data

x-idempotency-key: CD0305201705

x-jws-signature:

eyJhbGciOiJIJFQ0dPU1QzNDMxMCIsImtpZCI6IjFhYTRjZGFiODYwNGRjNzVjODZlZWZjMGJiYzVlMWI4YjBhNTE4ZjQzOTI3NmRhNDg5ZmVkYmI4OGUxYTFmYiJ9..iS37nUjBtJE7Hxg8JmOJw5purwIVnKltgOBHOZ4ghbkDbhtqbF7PoPzKniGw+yGmW0/2qGFWCat7bmKNwp/BVA==

Content-Type: application/json

```
{
  "Data":
  {
    "confirmation": "«Наименование Участника» настоящим подтверждает, что
в рамках удаленной идентификации клиентов с использованием системы ЦОИД
получено согласие ФИО, ИИН на обработку и передачу его (ее) персональных
данных третьим лицам."
  }
}
```

Описание заголовков запроса см. в приложении 2.

Response:

HTTP/1.1 200 OK

x-idempotency-key: CD0305201705

Content-Type: application/json

```
{
  "person": {
    "gender": {
      "nameRu": "Мужской",
      "code": 1,
      "nameKz": "Ер",
      "changeDate": "2013-09-19T09:44:33+06:00"
    }
  }
}
```

```

},
"documents": {
  "document": [
    {
      "number": "012345678",
      "beginDate": "2001-09-07",
      "patronymic": "ОМАРОВИЧ",
      "endDate": "2013-08-04",
      "surname": "ОМАРОВ",
      "name": "ШАЯН",
      "type": {
        "nameRu": "УДОСТОВЕРЕНИЕ РК",
        "code": "002",
        "nameKz": "ҚР ЖЕКЕ КУӘЛІГІ",
        "changeDate": "2013-09-19T09:45:40+06:00"
      },
      "birthDate": "1978-02-02",
      "issueOrganization": {
        "nameRu": "МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РК",
        "code": "002",
        "nameKz": "ҚР ІШКІ ІСТЕР МИНИСТРЛІГІ",
        "changeDate": "2013-09-19T09:45:40+06:00"
      }
    }
  ]
},
"citizenship": {
  "nameRu": "КАЗАХСТАН",
  "code": 398,
  "nameKz": "ҚАЗАҚСТАН",
  "changeDate": "2013-09-19T09:45:48+06:00"
},
"birthDate": "1978-02-02",
"iin": 000000000000,
"birthPlace": {
  "country": {
    "nameRu": "КАЗАХСТАН",
    "code": 398,
    "nameKz": "ҚАЗАҚСТАН",
    "changeDate": "2013-09-19T09:45:48+06:00"
  },
  "city": "АКТАУ",
  "district": {
    "nameRu": "АКТЮБИНСКАЯ",

```

```

    "code": 1904,
    "nameKz": "АҚТӨБЕ",
    "changeDate": "2013-09-19T09:45:41+06:00"
  },
  "foreignData": {
    "regionName": "АЛМАТИНСКИЙ"
  }
},
"surname": "ОМАРОВ",
"name": "ШАЯН",
"regAddress": {
  "country": {
    "nameRu": "КАЗАХСТАН",
    "code": 398,
    "nameKz": "ҚАЗАҚСТАН",
    "changeDate": "2013-09-19T09:45:48+06:00"
  },
  "beginDate": "2008-01-23",
  "city": "АКТАУ",
  "district": {
    "nameRu": "АКТАУ",
    "code": 1910,
    "nameKz": "АКТАУ",
    "changeDate": "2013-09-19T09:45:41+06:00"
  },
  "building": "153/8"
}
}
}

```

Описание заголовков ответа см. в приложении 3.

Описание полей тела ответа:

Поле	Тип	Описание
Iin	string	ИИН клиента
Surname	string	Фамилия
Name	string	Имя
Patronymic	string	Отчество
Gender	string	Пол
Nationality	string	Национальность
Citizenship	string	Гражданство
birthDate	DateTime	Дата рождения
Documents	array	Документы

Document	array	Массив документов
Name	string	Наименование документа
Number	string	Номер документа
issue_organization	string	Организация выпустившая документ
begin_date	DateTime	Дата документа
reg_address	object	Адрес прописки (регистрации постоянная и временная)
Country	string	Страна
District	string	Область
Region	string	Район
City	string	Населённый пункт
Street	string	Улица
Building	string	Номер дома
Corpus	string	Номер корпуса
Flat	string	Номер квартиры

6.4. Запрос на получение списка поставщиков алгоритма

Request:

GET https://onlinetest.kisc.kz/identity/1.1.0/vendors

Описание заголовков запроса см. в приложении 2.

Response:

HTTP/1.1 200 OK

```
{
  "vendors": [
    {
      "id": 1,
      "name": "VisionLabs"
    },
    {
      "id": 2,
      "name": "FORENSICS"
    }
  ]
}
```

Описание заголовков запроса см. в приложении 2.

Описание полей тела ответа:

Поле	Тип	Описание
vendors	object	

id	decimal	Идентификатор поставщика в Системе
name	string	Название поставщика алгоритма

6.5. Запрос на получение списка транзакций за указанный период

Request:

GET

<https://onlinetest.kisc.kz/identity/1.1.0/report/transactions/{fromDate}/{toDate}>

Описание заголовков запроса см. в приложении 2.

Параметр запроса (Переменная пути):

Поле	Тип	Описание
fromDate	string	Дата начала в формате ууууММдд
toDate	string	Дата окончания в формате ууууММдд

Response:

HTTP/1.1 200 OK

```
[{
  "vendor_name": "Verigram",
  "datetime": "24.09.2021 09:03:45",
  "similarity": 0.014690000000000002,
  "x_idempotency_key": "30db268b-438d-40cd-80d7-8e7ee2fe76f6"
}, {
  "vendor_name": "VisionLabs",
  "datetime": "24.09.2021 09:49:31",
  "similarity": 0.9959589839,
  "x_idempotency_key": "f7597db2-ee57-4ed6-b9d9-c4e5c4204ff6"
}, {
  "vendor_name": "Verigram",
  "datetime": "24.09.2021 10:01:08",
  "similarity": 0.014690000000000002,
  "x_idempotency_key": "c1650040-70cb-46d7-b56a-44c50c074a25"
}, {
  "vendor_name": "VisionLabs",
  "datetime": "24.09.2021 10:01:39",
  "similarity": 0.0,
  "x_idempotency_key": "8c6dfd0f-4df4-4f04-b01d-0962c6abc269"
}, {
  "vendor_name": "FORENSICS",
  "datetime": "24.09.2021 10:03:18",
  "similarity": 0.9773761034011841,
  "x_idempotency_key": "416b1f26-2b99-4939-b1ff-016fe7a193b9"
}]
```

Описание заголовков запроса см. в приложении 2.

В ответе на запрос возвращается массив с объектами. Поля объекта:

Поле	Тип	Описание
vendor_name	string	Наименование вендора
datetime	DateTime	Дата и время регистрации запроса
similarity	double	Степень сличения
x_idempotency_key	string	Уникальный идентификатор запроса

6.6. Запрос на получение JSON массива расшифровки к акту выполненных работ

Request:

GET https://onlinetest.kisc.kz/identity/1.1.0/report/actdetail/{year}/{month}

Описание заголовков запроса см. в приложении 2.

Параметр запроса (Переменная пути):

Поле	Тип	Описание
year	string	Год в формате YYYY
month	string	Месяц в формате ММ (без 0 в начале строки)

Response:

HTTP/1.1 200 OK

```
[
  {
    "date": "2022-01-01",
    "vendorName": "Verigram с 1 по 1000",
    "count": 1000,
    "price": 210.0,
    "amount": 210000.0
  },
  {
    "date": "2022-01-01",
    "vendorName": "Verigram с 1001 по 3000",
    "count": 1,
    "price": 111.0,
    "amount": 111.0
  },
]
```

```
{
  "date": "2022-01-01",
  "vendorName": "VisionLabs с 1 по 1000",
  "count": 1000,
  "price": 390.0,
  "amount": 390000.0
},
{
  "date": "2022-01-01",
  "vendorName": "VisionLabs с 1001 по 3000",
  "count": 1,
  "price": 204.0,
  "amount": 204.0
}
]
```

Описание заголовков запроса см. в приложении 2.

Описание полей элемента массива:

Поле	Тип	Описание
date	date	Операционная дата
vendorName	String	Наименование вендора с описанием тарифа
count	Int	Количество запросов
price	Float	Цена за один запрос
amount	Float	Сумма

6.7. Запрос на получение новостных уведомлений

Request:

GET https://onlinetest.kisc.kz/identity/1.1.0/news

Описание заголовков запроса см. в приложении 2.

Response:

HTTP/1.1 200 OK

```
[
  {
    "date": "2021-10-29",
    "subject": "касательно плановых работ на стороне АО \"НИТ\"",
    "text": "Здравствуйте!\nНастоящим АО «НПК» в рамках взаимодействия по проекту механизма удаленной идентификации, сообщает следующее. В период с
```

21:00 часов 30 октября по 09:00 часов 31 октября 2021 года будут проводиться плановые работы на стороне АО «Национальные информационные технологии». В этой связи, информируем Вас о возможных перебоях в работе системы Центра обмена идентификационными данными в вышеуказанный период.\n"

```
    },
    ...
]
```

Описание заголовков запроса см. в приложении 2.

В ответе на запрос возвращается массив с объектами. Поля объекта:

Поле	Тип	Описание
date	Date	Дата создания сообщения
subject	string	Тема сообщения
text	string	Текст сообщения

Приложение 1

Требование к изображениям

1. Изображение человека выше уровня груди;
2. изображение лица должно быть не менее 70% от общей площади фотоизображения;
3. голова должна быть повернута и наклонена на не более чем 8° от фронтального положения;
4. расстояние между центрами глаз при минимальном горизонтальном размере 480 пикселей должна составлять не менее 120 пикселей;
5. размер входного изображения должен быть не менее 640x480 пикселей и не более 4096x4096 пикселей;
6. изображение должно быть свободным от посторонних лиц в кадре;
7. плечи должны быть направлены к камере, исключая портретный стиль со взглядом через плечо;
8. лицо должно быть равномерно освещено без преобладающего направления света, с определенным соотношением интенсивности освещения;
9. изображение не должно содержать ярких пятен или бликов;
10. не допускается наличие головного убора. Необходимо обеспечить четкую видимость всех черт лица от подбородка до верхней линии лба, включая обе стороны лица;
11. разрешается использование очков только с прозрачными стеклами и без отражений вспышки. Окрашенные линзы запрещены. Необходимо

избегать использования очков с толстыми оправами, отдавая предпочтение моделям с тонкими и прочными оправами, если они необходимы субъекту. Оправа очков не должна перекрывать глаза, обеспечивая их полную видимость;

12. недопустимы световые артефакты или отражения вспышки;
13. взгляд должен быть направлен прямо в камеру;
14. глаза должны быть открыты и четко видны. Волосы не должны закрывать глаза;
15. выражение лица должно быть нейтральным;
16. фотография лица должна четкой, лицо в фокусе.

Заголовки HTTP запроса

Наименование заголовка	Значение	Обязательный	
		POST	GET
Content-Type	Стандартный HTTP заголовок; представляет Формат полезных данных, предоставляемых в запросе.	Да	Не используется
	Должен быть установлен в application/json.		
Асепт	Стандартный HTTP заголовок; Определяет тип содержимого, который требуется от сервера. Если задано, оно должно иметь значение: application/json.	Нет	Нет
x-idempotency-key	Пользовательский заголовок HTTP; Уникальный идентификатор запроса для поддержки идемпотентности. Цель этой возможности состоит в том, чтобы позволить Участникам повторять запросы API, которые завершились с таймаутом или неожиданной ошибкой.	Да	Не используется
x-jws-signature	JWS подпись полезной нагрузки запроса. Формирование заголовка описано в приложении 5.	Да*	Не используется

* Используется только в методе получения персональных данных п. 6.3.

Заголовки ответа

Наименование заголовка	Описание	Обязательный
Content-Type	Стандартный HTTP заголовок; представляет Формат полезных данных (payload – content), возвращаемых в ответе. НПК будет возвращать Content-type: application / json в качестве заголовка содержимого	Да
x-jws-signature	JWS подпись полезной нагрузки ответа	Да

Коды статусов ответа

Наименование	HTTP Статус	Описание	
Запрос завершен успешно	200 OK		
Запрос некорректный	400 Bad Request	Запрос сформирован не корректно, не переданы обязательные заголовки и иные данные. Так же возникает в случае истекшего сертификата или его отсутствия.	
Доступ к ресурсу API запрещен	403 Forbidden	Операции было отказано в доступе. Возникает в случае отсутствия у участника доступа.	
Запрашиваемый ресурс не найден	404 Not Found	No one person find! Possibly bad IIN	Возникает в случае когда по ИИН не найдено фото в ГБДФЛ
		Vendor not found	Вендор не найден
		SIMILARITY for Idempotency Key not found	Не найдена операция верификации для получения персональных данных
Участник попытался получить доступ к ресурсу с помощью метода, который не поддерживается	405 Method Not Allowed		
Не приемлемая операция	406 Not Acceptable	Возникает в случаях: повтор значения заголовка x-idempotency-key, запрос на персональные данные происходит по истечении 24 часов после проведения процедуры верификации а так же когда результат верификации ниже 85%, не соответствие требованиям к изображению в Приложение 1.	
Сбой в API	500 Internal Server Error	Возникает в случае проблем на стороне биометрического решения. Сюда так же относятся ошибки биометрического решения такие как:	

		на фото более 1 лица, лицо не распознано, не качественное изображение.	
Не доступен ГБДФЛ	523 Origin Is Unreachable	GBDFL is unavailable	Возникает в случае проблем на стороне интеграционной части, во время недоступности ГБДФЛ и/или АО «НИТ» при получении фото.
		Error obtaining KDP token	Возникает в случае проблем на стороне интеграционной части, во время недоступности КДП и/или АО «НИТ».
API не доступен	502 Bad Gateway		
Не доступен ГБДФЛ	504 Gateway Time Out	Возникает в случае проблем в интеграционной части, во время не доступности КДП или ГБДФЛ и/или АО «НИТ» при получение персональных данных.	

Формат ответа в случае ошибки:

```
{
  "timestamp": "2021-09-27T10:17:44.098+00:00",
  "status": 403,
  "error": "Forbidden",
  "path": "/identity/1.1.0/"
}
```

Описание полей тела ответа:

Поле	Тип	Описание
timestamp	dateTime	Дата и время ответа
status	int	Код HTTP статуса

error	string	Описание ошибки
path	string	Путь ресурса, в котором возникла ошибка

Формирование ЭЦП JWS

Для формирования ЭЦП необходимо выпустить регистрационные свидетельства в УЦ. Выпуск регистрационных свидетельств происходит в рабочем порядке совместно с технической поддержкой ЦОИД coid@kisc.kz.

В процессе формирования ЭЦП участвует необходимое программное обеспечение:

- 1) TumarCSP – крипто провайдер https://cms.npck.kz/downloads/res-open/tumar_others.htm
- 2) SDK – комплект библиотек, примеров кода для разработчика <https://cms.npck.kz/downloads/res-open/SDK.zip>
- 3) Регистрационные свидетельства (закрытый ключ) с алгоритмом ЭЦП ГОСТ 34.10-2015 РК. Алгоритм ГОСТ 34.310-2004 РК является устаревшим и в скором времени его поддержка будет исключена.

1: Подготовка данных.

Данными в запросе на получение персональных данных является тело запроса. Пример в п. 6.3.

2: Выбор алгоритма подписи.

Определите алгоритм, который будет использоваться для подписи. Например:

- ECGOST34310 - ГОСТ 34.310-2004 РК (deprecated);
- GOST3410-2015-512 - ГОСТ 34.10-2015 РК;

Для использования алгоритма ГОСТ 34.10-2015 РК необходимо использовать библиотеки и примеры кода из SDK.

3: Формирование заголовка (Header).

Header является JSON объектом, содержащим информацию о типе подписи и алгоритме состоящим из трех полей (параметров):

Параметр	Обязательный	Описание
alg	Да	Алгоритм, который используется при подписании.
kid	Да	Параметр указывает на то, чей ключ был использован для создания подписи. Должен соответствовать серийному номеру (SN) сертификата. Получатель должен использовать это значение для определения сертификата, используемого для проверки подписи.

iss	Нет	Эмитент регистрационных свидетельств. Должен соответствовать DN сертификата. Используется в случае работы с несколькими удостоверяющими центрами.
-----	-----	---

Пример Header:

```
{
  "alg": " GOST3410-2015-512",
  "kid":
"1a1c004f639577146e5704830b8106822028908d7cb32341fb9bf677feaa78bc"
}
```

4: Подписание данных

Подготовленные данные, тело запроса на получение персональных данных из примера п. 6.3 преобразуются в массив байт в кодировке UTF-8 и подписываются по примерам из SDK выбранным алгоритмом.

`signed = sign(byte(payload))`

5: Формирование JWS

JWS вычисляется как:

$$\text{JWS} = \text{BASE64URL}(\text{header}) + "." + \text{BASE64URL}(\text{payload}) + "." + \text{BASE64URL}(\text{signed})$$

В данном случае `payload = null`.

Пример готового JWS:

eyJhbGciOiJFQ0dPU1QzNDMxMCIsImtpZCI6IjFhMWMwMDRmNjM5NTc3MTQ2ZTU3MDQ4MzBiODEwNjgyMjAyODkwOGQ3Y2IzMjM0MWZiOWJmNjc3ZmVhYTc4YmMifQ==..RRGLuaDV5QpzSH367q5hQRKOYTQq8uUadEIViVsjDVk2Mv+PoA1vvLkVA1//FzLXIMOBAEycFFpSbb7PO7RZ1Q==

Проверка ЭЦП JWS

Ответы всех методов API содержат заголовок x-jws-signature. Для проверки подписи нужны то же программное обеспечение что и в приложении 5.

1: Получение подписанных данных

Тело каждого ответа является payload и подписано JWS. JWS содержится в заголовке x-jws-signature.

2: Парсинг JWS

Для парсинга JWS можно использовать открытые библиотеки, список которых приведен на сайте jwt.io либо самостоятельно разделить строку из заголовка x-jws-signature. Разделителем является символ точка «.». JWS состоит из трех частей:

- 1) Заголовок (Header): первая часть строки.
- 2) Полезная нагрузка (Payload): вторая часть строки. Обычно остается пустым так как полезной нагрузкой является тело ответа.
- 3) Подпись (Signature): третья часть строки.

3: Декодирование и проверка заголовка header

Каждая часть закодирована в формате Base64Url. Декодируйте их для анализа. Header является JSON объектом, содержащим информацию о типе подписи и алгоритме состоящим из трех полей указанных в приложении 5.

Необходимо проверить, какой алгоритм указан в поле alg. Проверка подписи происходит согласно алгоритму указанному в поле alg.

Получение открытого ключа происходит по значению поля kid.

4: Получение открытого ключа

Получить открытый ключ необходимо из LDAP УЦ. Для промышленной среды URL `ldap://ca.kisc.kz:62222` для ГОСТ 34.310-2004 РК и `ldap://ca.npsk.kz:62222` для ГОСТ 34.10-2015 РК.

Путь каталога (DN) аналогичен DN серверного сертификата. В списке сертификатов по пути необходимо найти сертификат у которого серийный номер соответствует значению из поля kid заголовка header.

Примеры работы с LDAP можно найти в SDK.

5: Проверка подписи

Используя полученный открытый ключ необходимо произвести проверку подписи согласно примерам из SDK.

Данными для проверки является тело ответа, подписью является третья часть JWS которую необходимо декодировать в байты.