

Памятка для взаимодействия с ИС ЦОИД

Этапы подключения к Тестовой среде:

Url ИС ЦОИД тестовой среды: onlinetest.kisc.kz Для ГОСТ 2015 onlinetest.kisc.kz:8243

1. Для взаимодействия с модулем ИС ЦОИД Участникам необходимо выпустить комплект криптографических ключей в Удостоверяющем Центре АО «НПК».

Для получения криптографических ключей для тестовой среды необходимо заполнить шаблон письма, который размещен на тестовом портале Удостоверяющего Центра в разделе «Инфо» по адресу: <https://betaca.kisc.kz/info> (ГОСТ 2004) или <https://betacms.npck.kz/info> для (ГОСТ 2015) Раздел «Инфо» (Пример сообщения для получения тестовых ключей и регистрационных свидетельств) и отправить на почту: supportca@kisc.kz

В заявлении необходимо указать алгоритм, на основе которого требуется выпустить комплект криптографических ключей (ГОСТ 2015 или ГОСТ 2004).

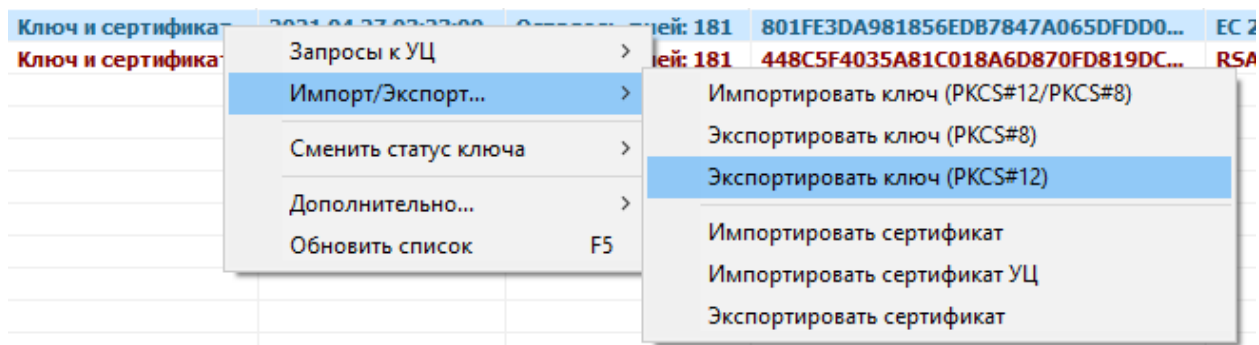
Комплект криптографических ключей первичной инициализации выпускается на 14 дней и их необходимо продлить на год. В случае возникновения вопросов касательно выпуска регистрационных ключей, в том числе продление, а также установка и настройка ПО «TumarCSP» необходимо обращаться по e-mail: supportca@kisc.kz или по телефону: **8 (727) 97-91-00**.

Для ГОСТ 2015 требуется новый Tumar конфигуратор, который использует новые алгоритмы и профайлы. Обновленную версию Tumar CSP можно скачать с сайта <https://cms.npck.kz>: кнопка «Инфо» → «Программное обеспечение, документация, примеры разработчикам» → «TumarCSP для пользователя», либо по прямой ссылке: <https://cms.npck.kz/downloads/res-open/client/TumarCSP.zip>

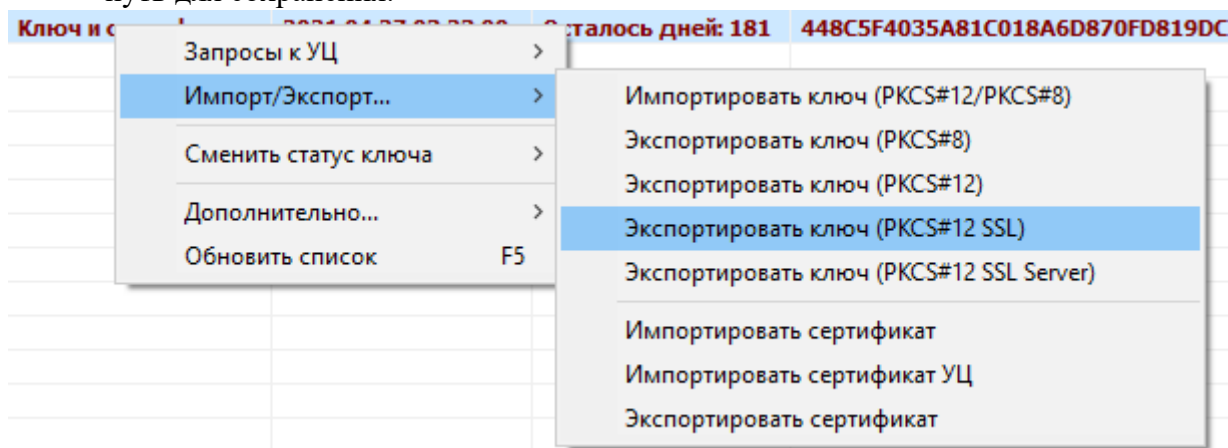
- Комплект криптографических ключей состоит из GOST и RSA сертификатов. **RSA (*.p12)** сертификат необходим для авторизации, а **GOST (*.pfx)** сертификат необходим для подписи.
- Для загрузки криптографических ключей необходимо запустить криптографический провайдер «TumarCSP» и перейти в профайл «FSystem», или «FSystem2015» для криптографических ключей ГОСТ 2015, в списке ключей должны отобразиться выпущенные криптографические ключи: **GOST (отображается синим цветом)** и **RSA (отображается красным цветом)**.

🔍 Список ключей: найдено 2					
Тип данных	Дата создания	Статус ключа	Серийный номер	Алгоритм	Экспортируемый ключ
Ключ и сертификат	2021.04.27 03:23:00	Осталось дней: 181	801FE3DA981856EDB7847A065DFDD...	EC 256/512 (GOST 34.310-2004 A...	Yes
Ключ и сертификат	2021.04.27 03:23:00	Осталось дней: 181	448C5F4035A81C018A6D870FD819D...	RSA 2048 (Xch) [1.3.6.1.4.1.6801....	Yes

- Для загрузки **GOST сертификата** необходимо его выделить, затем нажав на правую кнопку мыши в выпадающем меню выбрать пункт «Импорт/Экспорт...» и далее выбрать пункт «Экспортировать ключ (PKCS#12)», указать пароль и выбрать путь для сохранения.



- Для выгрузки **RSA сертификата** необходимо его выделить, затем нажав на правую кнопку мыши в выпадающем меню выбрать пункт «Импорт/Экспорт...» и далее выбрать пункт «Экспортировать ключ (PKCS#12 SSL)», указать пароль и выбрать путь для сохранения.



2. Для проведения тестирования в тестовой среде ИС ЦОИД Участникам необходимо направить официальное письмо на имя Председателя Правления АО «НПК» в произвольной форме. В письме необходимо указать, что в целях тестирования бизнес-процессов организации нужен доступ к промышленным данным для ИИН указанных в приложении в тестовой среде ИС ЦОИД. Реестр ИИН из тестовой группы содержит не более 10 **ИИН с указанием текста напротив каждого ИИН и ФИО «согласен на получение, хранение и обработку моих персональных данных третьими лицами» и подписью владельца ИИН-а.** Сканированный вариант необходимо направить на электронную почту канцелярии АО «НПК» по адресу: **info@kisc.kz**.

3. В Приложении представлены примеры по интеграции с использованием ПО «Postman».

Этапы подключения к Промышленной среде:

Url ИС ЦОИД: **online.kisc.kz** – промышленная среда. Для ГОСТ 2015 **online.kisc.kz:8443**

1. Регистрация участника в ИС ЦОИД произойдет автоматически после заключения договора, который расположен по адресу: <https://www.kisc.kz/wp-content/uploads/2024/01/czoid.-dogovor-s-uchastnikom-sopostavlenie-fotoizobrazhenij.docx>
Вкладка «Типовые договора» - «Договор с Участником (сопоставление фотоизображений)»

По всем вопросам касательно заключения договора необходимо обращаться в Управление ЦОИД по e-mail: coid@kisc.kz или по телефону: 8 (727) 297 91 44.

2. Для получения криптографических ключей в промышленной среде необходимо заполнить Приложение №1 Заявления/Соглашения к Договору о предоставлении услуг Удостоверяющего Центра в системах АО «НПК» (сам Договор прикладывать не надо, т.к. он является публичным, необходимо только Приложение №1) и скинуть Приложение для проверки корректности заполнения сотрудникам УЦ (без подписи, в Word файле) на e-mail: supportca@kisc.kz. **В заявлении необходимо указать алгоритм, на основе которого требуется выпустить комплект криптографических ключей «центр обмена идентификационными данными» (ГОСТ 2015 или ГОСТ 2004).** После подтверждения о правильном заполнении, необходимо подписать заполненное заявление, поставить печать и скан версию выслать на почту supportca@kisc.kz. После выпуска ключей сотрудниками УЦ Вы получите уведомление о готовности. Далее необходимо принести оригинал заявление нарочно в АО НПК, по адресу г.Алматы, мкр. Коктем 3, здание 21, 1 подъезд. При себе необходимо иметь удостоверение личности на имя получателя и флешку для записи ключей. Комплект криптографических ключей первичной инициализации выпускается на 14 дней и их необходимо продлить на год. Далее выпуск криптографических ключей производится на портале УЦ АО «НПК» по адресу: <https://ca.kisc.kz/auth> (ГОСТ 2004) или <https://cms.npck.kz/auth> (ГОСТ 2015) – для промышленной среды.

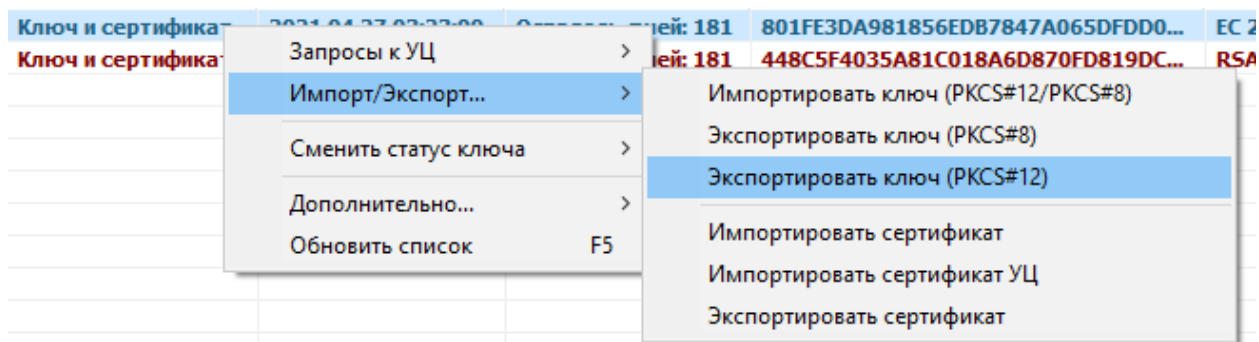
В случае возникновения вопросов касательно выпуска регистрационных ключей, в том числе продление, а также установка и настройка ПО «TumarCSP» необходимо обращаться по e-mail: supportca@kisc.kz или по телефону: 8 (727) 97-91-00.

Для ГОСТ 2015 требуется новый Tumar конфигуратор, который использует новые алгоритмы и профайлы. Обновленную версию Tumar CSP можно скачать с сайта <https://cms.npck.kz>: кнопка «Инфо» → «Программное обеспечение, документация, примеры разработчикам» → «TumarCSP для пользователя», либо по прямой ссылке: <https://cms.npck.kz/downloads/res-open/client/TumarCSP.zip>

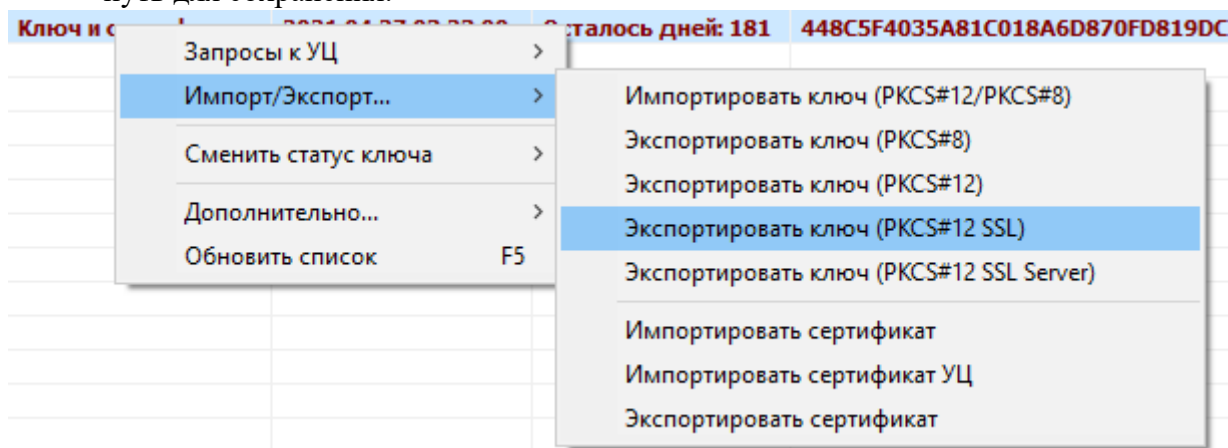
- Комплект криптографических ключей состоит из GOST и RSA сертификатов. **RSA (*.p12)** сертификат необходим для авторизации, а **GOST (*.pfx)** сертификат необходим для подписи.
- Для загрузки криптографических ключей необходимо запустить криптографический провайдер «TumarCSP» и перейти в профайл «FSystem» (для ГОСТ 2004), или «FSystem2015» для (ГОСТ 2015). В списке ключей должны отобразиться выпущенные криптографические ключи: **GOST (отображается синим цветом)** и **RSA (отображается красным цветом)**.

🔍 Список ключей: найдено 2					
Тип данных	Дата создания	Статус ключа	Серийный номер	Алгоритм	Экспортируемый ключ
Ключ и сертификат	2021.04.27 03:23:00	Осталось дней: 181	801FE3DA981856EDB7847A065DFDD...	EC 256/512 (ГОСТ 34.310-2004 A...	Yes
Ключ и сертификат	2021.04.27 03:23:00	Осталось дней: 181	448C5F4035A81C018A6D870FD819D...	RSA 2048 (Xch) [1.3.6.1.4.1.6801....	Yes

- Для загрузки **GOST сертификата** необходимо его выделить, затем нажав на правую кнопку мыши в выпадающем меню выбрать пункт «Импорт/Экспорт...» и далее выбрать пункт «Экспортировать ключ (PKCS#12)», указать пароль и выбрать путь для сохранения.



- Для выгрузки **RSA сертификата** необходимо его выделить, затем нажав на правую кнопку мыши в выпадающем меню выбрать пункт «Импорт/Экспорт...» и далее выбрать пункт «Экспортировать ключ (PKCS#12 SSL)», указать пароль и выбрать путь для сохранения.



Доступ к промышленной среде ИС ЦОИД осуществляется через выделенный канал связи посредством IP VPN или IPSEC (процедура получения ключей для туннеля IPSEC аналогична процедуре получения ключей для ЦОИД, только в заявлении необходимо выбрать пункт «туннель (IPsec)».

Для подключения через IP VPN необходимо заполнить шаблон письма: <https://www.kisc.kz/wp-content/uploads/2023/06/shablon-dlya-podcluc-kanala-ip-vpn-rus.docx>

Для подключения через IPSEC необходимо заполнить шаблон письма: <https://www.kisc.kz/wp-content/uploads/2023/06/shablon-ipsec-rus.docx>

Сканированный вариант заполненного шаблона письма необходимо направить на электронную почту канцелярии АО «НПК» по адресу: info@kisc.kz

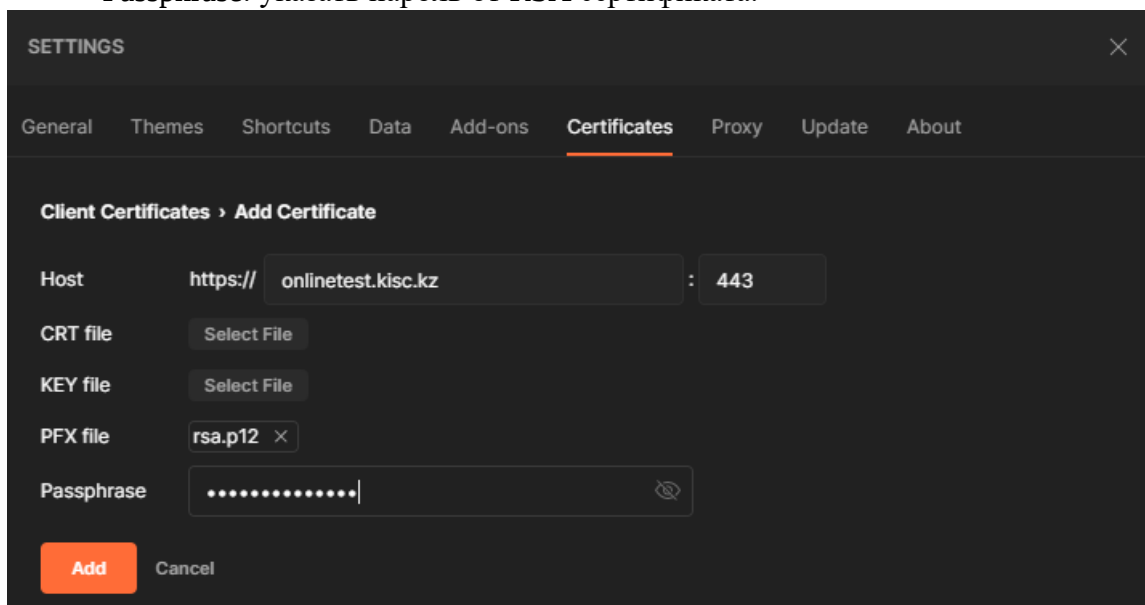
3. Утвержденные тарифы АО «НПК» для предоставления услуг в ИС ЦОИД размещены на сайте АО «НПК» по адресу: <https://www.kisc.kz/pcid/> Вкладка «Тарифы».

4. В Приложении представлены примеры по интеграции с использованием ПО «Postman».

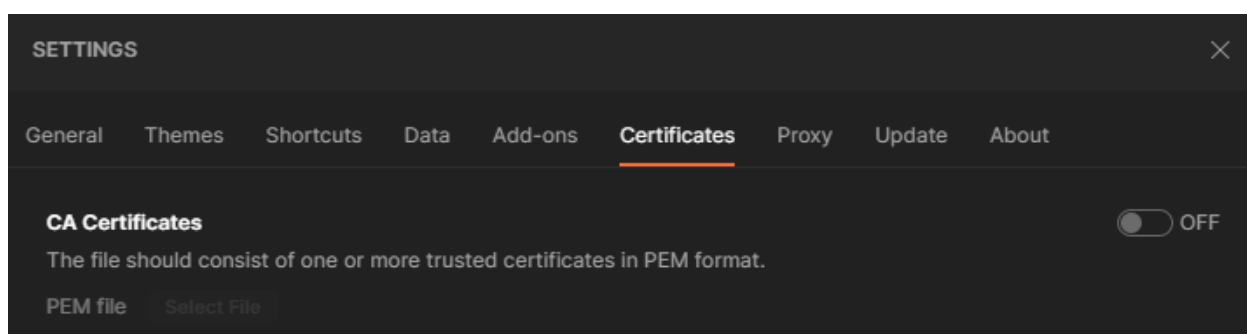
Ниже представлены примеры по интеграции с использованием ПО «Postman».

1. Для доступа к API необходимо добавить криптографические ключи в ПО «Postman». Для этого необходимо перейти в настройки (Settings), раздел «Certificates», далее нажать на кнопку «Add Certificate» и указать следующие параметры:

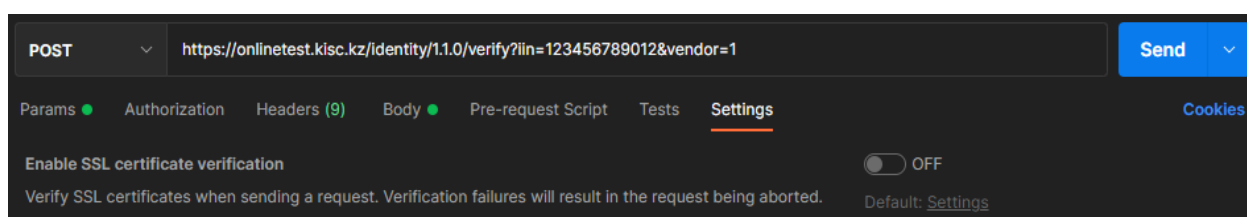
- Host: onlinetest.kisc.kz:443;
- PFX file: указать путь до RSA сертификата;
- Passphrase: указать пароль от RSA сертификата.



Для добавления нажать на кнопку «Add». Также необходимо отключить проверку сертификатов. Для этого необходимо перейти в настройки (Settings), раздел «Certificates» и в разделе «CA Certificates» установить значение переключателя в положение «OFF».



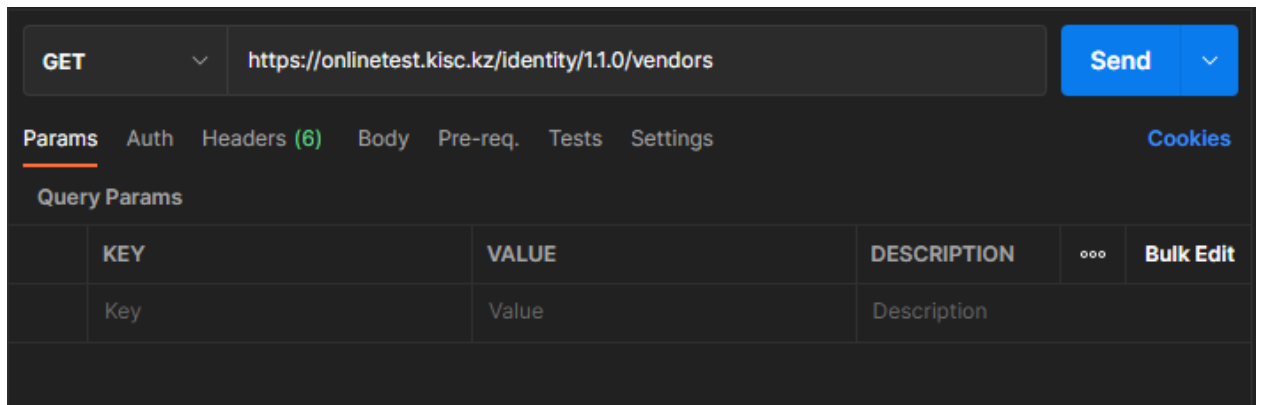
Также в настройках запроса на вкладке «Settings» в разделе «Enable SSL certificate verification» установить значение переключателя в положение «OFF».



2. Запрос на получение списка вендоров

Метод: GET

Url: <https://onlinetest.kisc.kz/identity/1.1.0/vendors>



KEY	VALUE	DESCRIPTION
Key	Value	Description

Ответ:

```
{
  "vendors": [{
    "id": 1,
    "name": "VisionLabs"
  }, {
    "id": 2,
    "name": "FORENSICS"
  }, {
    "id": 3,
    "name": "Verigram"
  }, {
    "id": 4,
    "name": "Biometric.kz"
  }, {
    "id": 5,
    "name": "BTSDigital"
  }
]}
```

3. Запрос на верификацию

Метод: POST

Url: <https://onlinetest.kisc.kz/identity/1.1.0/verify?iin={iin}&vendor={vendor}>

Request Params:

- iin – ИИН клиента
- vendor – id код вендора

Headers:

- x-idempotency-key – уникальный идентификатор x-idempotency-key
- Content-Type - image/png тип данных

Body: фотоизображение в binary

POST

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

Send

Params

Auth

Headers (9)

Body

Pre-req.

Tests

Settings

Cookies

Query Params

	KEY	VALUE	DESCRIPTION	...	Bulk Edit
☒	iin	123456789012			
☒	vendor	1			

Ответ:

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

4. Запрос на получение персональных данных

Метод: POST

Url: https://onlinetest.kisc.kz/identity/1.1.0/personel_data
https://onlinetest.kisc.kz/identity/1.1.0/personal_data
<https://onlinetest.kisc.kz/identity/1.1.0/data>

Headers:

- x-idempotency-key – идентификатор x-idempotency-key запроса на верификацию
- Content-type – application/json
- x-jws-signature – сгенерированная из body подпись

Body: текст согласия клиента на получение и обработку персональных данных третьими лицами

POST

<https://onlinetest.kisc.kz/identity/1.1.0/data>

Send

Params

Auth

Headers (11)

Body

Pre-req.

Tests

Settings

Cookies

Query Params

	KEY	VALUE	DESCRIPTION	...	Bulk Edit
	Key	Value	Description		

Ответ:

Полный перечень возвращаемых персональных данных описан в технической документации на сайте <https://www.kisc.kz/pcid/> Вкладка «Техническая документация».

Примечание:

Если передать параметр **mcdb=1** (<https://onlinetest.kisc.kz/identity/1.1.0/data?mcdb=1>), в этом случае с персональными данными клиента в поле **mobilephone** будет возвращен номер телефона зарегистрированный в базе мобильных граждан.

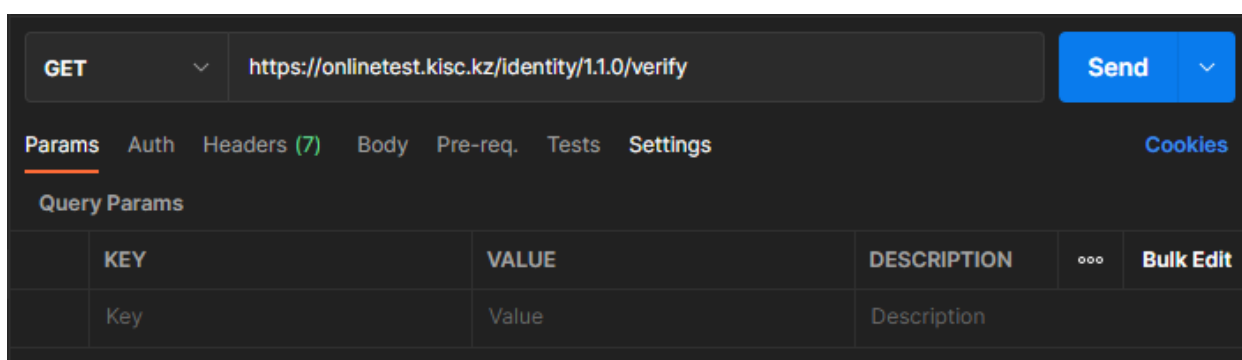
5. Запрос на получение повторного результата верификации

Метод: GET

Url: <https://onlinetest.kisc.kz/identity/1.1.0/verify>

Headers:

- x-idempotency-key – идентификатор x-idempotency-key запроса на верификацию



KEY	VALUE	DESCRIPTION
Key	Value	Description

Ответ:

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

6. Запрос на получение новостных уведомлений

Метод: GET

Url: <https://onlinetest.kisc.kz/identity/1.1.0/news>

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

Params
Auth
Headers (6)
Body
Pre-req.
Tests
Settings
Cookies

Query Params

	KEY	VALUE	DESCRIPTION	...	Bulk Edit
	Key	Value	Description		

Ответ:

```
[
  {
    "date": "2021-10-29",
    "subject": "касательно плановых работ на стороне АО \"НИТ\"",
    "text": "Здравствуйте!\nНастоящим РГП «Казахстанский центр межбанковских расчетов Национального Банка Республики Казахстан» 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"
  },
  ...
]
```

7. Запрос на получение списка проведенных транзакций за период

Метод: GET

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

URL Variables:

- fromDate – Начальная дата в формате YYYYMMDD
- toDate – Конечная дата в формате YYYYMMDD

GET
https://onlinetest.kisc.kz/identity/1.1.0/report/transactions/20211028/20211029
Send

Params
Auth
Headers (6)
Body
Pre-req.
Tests
Settings
Cookies

Query Params

	KEY	VALUE	DESCRIPTION	...	Bulk Edit
	Key	Value	Description		

Ответ:

```
[
  {
    "vendor_name": "VisionLabs",
    "datetime": "28.10.2021 11:20:40",
    "similarity": 0.9959589839,
    "x_idempotency_key": "402735df-236d-40d7-a785-2f17e95550c4"
  }, {
    "vendor_name": "FORENSICS",
    "datetime": "29.10.2021 10:20:52",
    "similarity": 0.0,
    "x_idempotency_key": "f97c33e8-8f83-473b-8b26-8980b92d38c0"
  }
  ...
]
```

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

Метод: GET

Url: <https://onlinetest.kisc.kz/identity/1.1.0/report/actdetail/{year}/{month}> URL Variables:

- year – Год в формате YYYY
- month – Месяц в формате ММ (без 0 в начале строки)

GET <https://onlinetest.kisc.kz/identity/1.1.0/report/actdetail/2022/01> Send

Params Authorization Headers (6) Body Scripts Settings Cookies

Query Params

	Key	Value	Description	...	Bulk Edit
	Key	Value	Description		

Ответ:

```
[
  {
    "date": "2022-01-01",
    "vendorName": "Verigram с 1 no 1000",
    "count": 1000,
    "price": 210.0,
    "amount": 210000.0
  },
  {
    "date": "2022-01-01",
    "vendorName": "Verigram с 1001 no 3000",
    "count": 1,
    "price": 111.0,
    "amount": 111.0
  },
  {
    "date": "2022-01-01",
    "vendorName": "VisionLabs с 1 no 1000",
    "count": 1000,
    "price": 390.0,
    "amount": 390000.0
  },
  {
    "date": "2022-01-01",
    "vendorName": "VisionLabs с 1001 no 3000",
    "count": 1,
    "price": 204.0,
    "amount": 204.0
  }
]
```