Инструкция для получения токена в АРІ ИС МПТ

Необходимые условия

- ✓ Наличие установленного программного обеспечения NCALayer.
- ✓ SDK НУЦ, для получения необходимо обратится в НУЦ РК . Адрес портала: https://pki.gov.kz/
- ✓ После получения SDK НУЦ необходимо пройти по следующему пути внутри папки (SDK\NCALayer\commonbundle_sample\index.html)
- ✓ При отсутствии возможности получения SDK НУЦ, вы можете воспользоваться плагинами WebSocket Client для браузеров (например плагин Simple Web Socket Client для Chrome или Mozilla).
- ✓ Ссылка к приложению WebSocket Client : https://chrome.google.com/webstore/detail/simplewebsocket-client /pfdhoblngboilpfeibdedpjgfnlcodoo
- ✓ Данные для подписания (например поле data ответа при запросе авторизации).

Шаги: Шаг №1 Метод GET /auth/key

Описание запроса:

Параметр	Значение
URL	<url стенда="">/auth/key</url>
Метод	GET

интернет-магазин ch	hrome		
Разные > Расширения >	Simple WebSocket Client		
Simple V	VebSocket Client 796 🛈 Инструменты разработчика Пользователей: 100 000+	Удалить из Chrome	
Обзор	Меры по обеспечению конфиденциальности Отзывы	Поддержка Похожие	
	Server Location URL: ws://echo websocket.org Status: OPENED Request Helio from Simple WebSocket Client Send [Shortcut] Ctr + Enter		
	Message Log Clear Hello from Simple WebSocket Client Hello from Simple WebSocket Client		

A My Wor	kspace	New Import	GET https://stage.ismet.kz/		No Environment v ©
Collections	+ =	000	https://stage.ismet.kz/api/v3/true-api/auth/key		🖺 Save 🗸 🆉 🖾 🌾
oo APis	GET New Request		GET v https://stage.ismet.kz/api/v3/true-api/auth/ki	ey st Script Tests Settings	Send v Cookies
Environments			KEY Key	VALUE	DESCRIPTION ••• Bulk Edit
전 Monitors 더 ⁰ Flows					
4) History			Body Cookies Headers (5) Test Results	🔁 Status: 40	00 Bad Request Time: 75 ms Size: 235 B Save Response V

Принимаемые параметры:

Параметр	Описание	Тип	Обязательность
UUID	Уникальный идентификатор сгенерированных случайных данных	String	Да
data	Случайная строка данных в формате BASE64	String	Да

Пример полученного ответа:

History	Body Cookies Headers (7) Test Results	Status: 200 OK Time: 64 ms Size: 289	B Save Response V
	Pretty Raw Preview Visualize JSON V 🚍		r q
	1 2 *uuid*: *84d9f886-8a92-433d-a86b-aa978a45ff16*, *data*: *GWFPTMZMJYEDQMAVYHOWLLXFRAAKFW*		I
E Q. Find and Replace D Console		🕲 Cookies 🧬 Capture requests 🧐 Bootcamp	🗈 🗈 Runner 🗊 Trash 💀

Данные из поля **uuid** - будут использованы в 4 шаге; данные из поля **data** - будут использованы в 2 шаге.

Шаг №2 Кодирование данных в Base64

Кодирование данных из поля data полученного в первом шаге в формат Base64.

Пример конвертации с помощью онлайн pecypca https://www.base64encode.org/

\leftrightarrow \rightarrow C (a) base64encode.org	Ē ★	* = 0	
Encode to Base64 format Since and a ware data than push the accords button.	★ Bonus tip: Bookmark us!		
	Other tools		
GWFPIM2MJYEDQMAVYHOWLLXFRAAKFW	URL Decode		
	URL Encode		
Данные из поля data	JSON Minify		
	JSON Beautify	6	
S. C. Car	JS Minify	Ø	
	JS Beautify	0	
• To encode binaries (like images, documents, etc.) use the file upload form a little further down on this page.	CSS Minify	۲	
UTF-8 V Destination character set.	CSS Beautify		
CRLP (Windows) CRLP (Windows)	☆ Partner sites		
Spit lines into 76 character wide chunks (useful for MIME).	Number System Converter	=	
Perform URL-safe encodingeruses Base64URL format)	TV Show and Movie Ratings	R	
Live mode OFF Encodes in real-time as you type t base64	Secure Group Chat	Ũ	
> ENCODE < Encodes your data into the area below			
RIdGUFRNWk1KWUVEUU1BVIIIT1dMTFhGUkFBS0ZX			
			C

Шаг №3 Подписание данных

Подписание данных инструментами SDK НУЦ.

Страница index.html из папки commonbundle_sample из пакета SDK НУЦ:

\leftrightarrow \rightarrow C (Файл C:/commonbundle_sample/index	chtml	Ŕ	\$ * =	
Пр	имеры использования методов NCALayer			
Выберите необходимый т	ип носителя Добавить доступные токены			
PKCS12		\$		
1. Данные клю	ча			
Получить данные ключа				
Алиас ключа	Alias			
Идентификатор ключа	keyld			
Алгоритм ключа	algorithm			

С использованием метода №5 "Подпись Base64 данных в формате CMS" SDK НУЦ закодированные в base64 данные подписываем с включением данных в подпись():

R1dGUFRNWk1KWUVEUU1BVllIT1dMTFhGUkFBS0Z>	X		
		4	
Включить данные в подпись			
Подписать			
MIII3wYJKoZIhvcNAQcCoIII0DCCCMwCAQExDzANBg 0ZXoIIGRzCCBkMwggQroAMCAQICFEsH3L3/+qtVlz4 0KLQotCr0pog01rQo90Y0JvQkNCd0JTQq9Cg0KPQq VowgYUxJDAiBgIVVBAMMG50oJXQmtCY0JzQntCS1 NTM1MTY4NTELMAKGA1UEBhMCS1oxHTAbBgNVB/ AgPvuE8A0VGMT92yHSJYWIZeKP69/YHo35dlbTs11	JlghkgBZQMEAgEFADAtBgkqhkiG9w0BJ 4VvLxVMli11CfZMA0GCSqGSlb3DQEBC (NCrINCe0KDQotCQ0JvQq9KalChSU0Ep INCg0KPQodCi0JDQnDEXMBUGA1UEB/ CoMFNCU0JDQndCY0K/QoNCe0JLQmN &MMMH7Mvb3A4ySWtPldYMqFivKBGP	BwGgIAQeR1dGUFRNWk1KWUYEU wUAMFIxCzAJBgNVBAYTAktaMUMv iMB4XDTIyMDIyNDA3MDAwMVoXE wOOK(gildca0jQnNCc0JixGDAWB cOnMIIBijANBgkqhkiG9w0BAQEFAA XUsOKRLi2kVZxe220ZX26282SoE	J1BVIIIT1dMTFhGUkFBS vQQYDVQQDDDrSsNCb JTI2MDIyNDA3MDAwM JNVBAUTD0IJTjkyMDUy OCAQ8AMIBCgKCAQE J0HsnYbWmJDNsfobldi

В результате получаем данные, которые будут использованы в 4 шаге для получения токена.

Подпись с помощью плагина браузера.

Альтернативным методом подписания данных является использование плагина для Web браузера. На примере будет использован плагин **Simple WebSocket Client**, доступный для скачивания в Интернет-магазине Chrome.

Необходимо запустить плагин и создать подключение по адресу: wss://127.0.0.1:13579/

C Simple WebSocket Client chrome-extension://pfdhobIngboilpfeibdedpjgfnlcodoo/index.html	Ē	☆	*	≡J		
Server Location Open URL: [wss://127 0.0.1:13579] Open Status: CLOSED Open						
Request A Send [Shortcut] Ctr + Enter						
Message Log Clear						

Выполнить запрос в **WebSocket Client** с подстановкой кодированных в **Base64** данных на *шаге 2* в поле **SIGNATURE** и подписать используя сертификат для подписи:

Пример запроса:

```
{
    "module": "kz.gov.pki.knca.commonUtils",
    "method": "createCMSSignatureFromBase64",
    "args": [
        "PKCS12",
        "SIGNATURE",
        "UkhZRVJMV0FWVUZGV0pMRVhRVE5BVkhGTU1BQ1RU",
        true
    ]
}
```



В результате чего будет получены подписанные данные:



Данные из поля responseObject - будут использованы в следующем шаге.

Шаг №4 Метод POST /auth/simpleSignIn

Получение токена методам POST /auth/simpleSignIn

Метод предназначен для получения аутентификационного токена по ЭЦП.

Описание запроса:

Параметр	Значение
URL	<url стенда="">/auth/simpleSignIn</url>
Метод	POST
Content- Type	application/json

Передаваемые параметры:

Параметр	Значение	Тип	Обязательность
UUID	Уникальный идентификатор подписанных случайных данных	String	Да
data	Подписанные ЭЦП зарегистрированного УОТ - случайные данные в формате BASE64	String	Да

Пример запроса:

Collections	+ =	000	https://stage.ismet.kz/api/v3/true-api/auth/simpleSignIn	🖺 Save 🗸 🏉	
00 APIs	GET New Request		POST v https://stage.ismet.kz/api/v3/true-api/auth/simpleSignIn	Send v	: (f)
			Params Authorization Headers (9) Body Pre-request Script Tests Settings	Cookies	
Environments			🜑 none 🔍 form-data 🔍 x-www-form-urlencoded 🛑 raw 🔍 binary 🔍 GraphQL JSON 🗸	Beautify	
Mock Servers Monitors H ^{CI} Flows			1 2 3 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	UIBVIIITIdMTFhGUKFBS9ZX0IIGRZCCBKMw x0Y83vQkHcd0JTQq9cg8KPQqHcIINc86KDQo xSINCg8KPQodcI0JQnDEXMBUGA1UEBxw08K x7X257pyc5N0f7P13ZueQF±j3Pc y5vgWtU6hFuroZL9MYaxM5YxD0M	
History			Response	~	

Поле **uuid** – данные, полученные на 1 шаге; поле **data** – данные, полученные на 3 шаге.

Пример успешного ответа:

History	Body Cookies (1) Headers (9) Test Results					Status: 200 OK Time: 231 ms Size: 5.55 KB Save Response
	Pretty	Raw Preview	Visualize	JSON \vee	⇒	rd of
	1 4	"token": "eyJhb eyJacm9Kub VayOucUSUp URBLX7800 QUBLX1002 URBL100 URFX1800 WRST800 PULRFUISI ODUILCJM000	SciOiJIUzIIN 9X2dyb3VwX21 UEFOVCISIIdI IRJ001Q0U5UI FOVCJdfSx7Tm PTEVTQUXFUII 201QQUSUIIM EFSVELDSVBBT RSQURFX1BBUI 10JYWMDAwMDI	iIsInR5cCI6 uZm8iOlt7Im TÖXFUØFMRVI iwiVØhPTEVT ShbWUiOiJwa sIk1FRELOQU VØhPTEVTQUX lQiLCJXSE9M RJQ@IQQU5UI 90SwiYXV@aG	IkpXVCJ9 5hbWUiOi 1XX0seyJ QUxFUiJd GFybWEiL wiXX0sey FUIJdfSx RVNBTEVS iwiV0hPT 9yaXRpZX	hbGNvaG9sIlwic3RhdHV2IjoINSISInR5cGV2IjpbIJJFVEFJTCISIIBST0RVQ0VSIIwISUJQTJURVIILCJUUKFER uvMIIJjoId2F02XILCJ2GF00XM10IIIIwIdHnzXM10ISUFJRFV0RVIILCJSRVRSUwILCJJTV9PUIRFUISII 15X7mshbMuljJatkkrIWic3BndHvZj0ISISIISIA65C0XIjDIIST8RVQ0VSIiwISUJQTJURVIILCJUKFER9 CJ2dGF00XM10IIIIwidHlwZXM10ISIUKVUQUIMImIwIFJPRFVDRVIILCJTVBPUIRFUISIISUJQTUBVIILCJUKFER9 JumAIIjoInHALCJ2dGF00XM10IIII@0HlwZXM10ISUFJRFV0RVIILCJSRVRSUwILCJJTVBPUIRFUISIIRS0 JumAIIJOINHALCJ2dGF00XM10IIII@0HlwZXM10ISUFJRFV0RVIILCJSRVRSUWILCJJTVBPUIRFUISIIRS0 IJn6hbul0JJ200501y5InMv8XR10fIJUICJ00x812Jf00XJ0UKEVUNFUISIJJVEFJTCILLSJRVRSSUMILCJJTVB9 IJ19LHSUMFZSIGIRVFY12SIGL02dGf00XM10IIIImidHlwZXM10ISUFJRFVDRVIILCJSRVRSUMILCJJTVB7 H10F00XUJ2GF0510VZZXJC25RH4VZ10J0UKVZVEImidXM120VXIIJf00KKSLC2D9M210IEM9AHVUZVTE2 H10Is0J3QVCILTSIPUKRFUJMUTJERVTRKF0QURFLUNPTIRST0XMVIUTU9ESUZZSUSHLIdSSVRFIIm10J3QVC100
Generation Console						🕓 Cookies 🧬 Capture requests 😁 Bootcamp 🗉 Runner 前 Trash 🔛

В ответ получаем авторизационный токен.