

## ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «CRYPTOSOCKET»

## Инструкция по установке в ОС macOS

Прочие документы 398-980340000290.CS 90.01.24011870 Листов 20

# Содержание

1 Аннотация	
2 Общие сведения	
2.1 Наименование и обозначение	4
2.2 Производитель	4
2.3 Назначение	4
2.4 Минимальные требования к техническим средствам	4
2.5 Требования к программному обеспечению	4
	-
3 установка CryptoSocket и ПО «1 у МАР-СSР»	
4 Установка драйвера KAZTOKEN	7
5 Установка SSL-сертификата в хранилище	
6 Просмотр устройствя хрянения ключей и сертификатов	
	15
	•••••••••••••••••••••••••••••••••••••••
	10
/ Список плагинов поддерживаемых в CryptoSocket	
8 Выход из CryptoSocket	

#### 1 Аннотация

Программное обеспечение «CryptoSocket» (далее – CryptoSocket) предназначено для обеспечения безопасного взаимодействия пользователей с информационными системами через веб-интерфейсы в режиме реального времени с использованием надежных методов криптографической защиты информации.

СтуртоSocket позволяет организовать использование ЭЦП при работе в любом из предпочитаемых пользователем распространенных браузеров в различных операционных системах; организовать ее применение для аутентификации с использованием биометрической информации, а также с использованием носителей ключевой информации; организовать взаимодействие с любым из аккредитованных в РК удостоверяющим центром.

В инструкции приводятся сведения по установке и использованию программного обеспечения «CryptoSocket» (далее - CryptoSocket).

## 2 Общие сведения

#### 2.1 Наименование и обозначение

Наименование: Программное обеспечение «CryptoSocket» Обозначение: CryptoSocket

#### 2.2 Производитель

ТОО «НИЛ «Гамма Технологии»

Адрес: пр. Абая 20/14, оф.1, г. Алматы, Республика Казахстан, А15Е1Н5

Тел: 267-20-61

E-mail: info@gamma.kz

#### 2.3 Назначение

Организация криптографической поддержки веб-браузеров с помощью программного средства криптографической защиты информации «ТУМАР-CSP».

#### 2.4 Минимальные требования к техническим средствам

- Процессор (CPU): Intel Core2 E6400.
- Оперативная память (RAM): 4Gb.
- Свободное место на жестком диске: 2Gb.

#### 2.5 Требования к программному обеспечению

Поддерживаемая операционная система: macOS: Catalina 10.15, Big Sur, Monterey, Ventura.

Для работы CryptoSocket должно быть установлено средство криптографической защиты информации «ТУМАР-CSP».

Поддерживаемые веб-браузеры:

- Google Chrome версии 60.0.3112.113 и выше;
- Safari.

## 3 Установка CryptoSocket и ПО «ТУМАР-CSP»

Для установки CryptoSocket и ПО «ТУМАР-CSP» на рабочую станцию:

1. Нажмите правой кнопкой мыши на файл с дистрибутивом TumarCSPInstall.app и выберите Открыть в приложении → Установщик (по умолчанию).

•••	< > Setup	≔≎			$\bigcirc$	··· •	Q
Избранное	Имя	<ul> <li>Дата изменения</li> </ul>		Размер		Тип	
🧑 AirDrop	TumarCSPInstall_sig			8 1	0,7 MB	Архивпа	акета
🕘 Недавние		Открыть					
🙏 Программы		Открыть в приложении	>	Установш	ик (по	умолчанию	<b>)</b>
📃 Рабочий стол		Переместить в Корзину		App Store			
Documents		Свойства		Другое			
🕹 Загрузки		Переименовать Сжать «TumarCSPInstall signed.pkg»					
Места		Дублировать					
iCloud Drive		Создать псевдоним					
⊖ Firefox ≜		Быстрый просмотр					
Теги		Скопировать					
• Красный		Поделиться	>				
<ul> <li>Оранжевый</li> </ul>							
🕒 Желтый		Теги					
A second second second second		Быстрые действия	>				
	and the second s	Отправить файлы с помощью TeamViewer					

Рисунок 1. Запуск мастера установки

**2.** В окне мастера установки нажмите на кнопку **Продолжить**. При необходимости введите пароль администратора операционной системы.

CryptoSocket Installer
установить Ооновить удалить Выход

Рисунок 2. Начало установки CryptoSocket

**3.** Дождитесь завершения установки CryptoSocket, ПО «ТУМАР-CSP» и сертификатов. Нажмите на кнопку **Выход**.

The right ha Install proce	s been granted ss run CSP process			
kill CryptoSo change TUN change Cry	ocket process MAR_CSP otoSocket			
CryptoSock	et is successfully i	nstalled		

Рисунок 3. Установка CryptoSocket успешно завершена



## **4 Установка драйвера КАZTOKEN**

Для установки драйвера КАΖТОКЕМ на рабочую станцию:

1. После завершения установки CryptoSocket автоматически откроется окно загрузки модулей для работы с устройствами KAZTOKEN. Чтобы начать установку нажмите на кнопку **Продолжить**.



Рисунок 4. Начало установки драйвера KAZTOKEN

2. Выберите место для установки и нажмите на кнопку Продолжить.



Рисунок 5. Выбор места установки драйвера KAZTOKEN

3. Для установки драйвера КАΖТОКЕН нажмите на кнопку Установить.



Рисунок 6. Стандартная установкадрайвера KAZTOKEN на Macintosh HD

4. Дождитесь завершения установки драйвера КАΖТОКЕΝ и нажмите на кнопку Перезагрузить.



Рисунок 7. Установка драйвера KAZTOKEN успешно завершена

5. Запустите CryptoSocket. В системном трее появится значок CryptoSocket.



Рисунок 8. Значок CryptoSocket в системном трее



### 5 Установка SSL-сертификата в хранилище

Для работы с CryptoSocket необходимо установить SSL-сертификат в хранилище Keychain Access (Связка ключей).

Для установки SSL-сертификата в хранилище Keychain Access:

1. Откройте Launchpad, в строке поиска укажите Keychain.

C keychain C C key	

Рисунок 10. Значок «Связка ключей» в Launchpad

- 2.
- Нажмите на значок 🅅 (Keychain или Связка ключей).
- 3. Нажмите на кнопку Вход в левой части меню, выберите сертификат ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA) и нажмите на него 2 раза:

Связка ключей		Ď i	Q Поиск	
Все объекты Пароли Секретные заметки Мо	и сертификаты Ключи Се	отификаты		
Сенфика Макериание бюро сертификации Истекает: среда, 25 июня 2025 г. в 10 Оданный сертификат помечен как на	ТАЛЫҚ (RSA) :26:36 Восточный Казахстан, с эдежный для этой учетной зап	стандартное время иси		
Имя	^ Тип	Дата изменения	Срок действия	Связка ключей
127.0.0.1	Сертификат		22 марта 2023 г., 10:15:33	Вход
[7] НЕГІЗГІ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA)	Сертификат		27 июля 2025 г., 11:22:53	Вход
📷 ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA)	Сертификат		25 июня 2025 г., 10:26:36	Вход
	Связка ключей Все объекты Пароли Секретные заметки Мо	Связка ключей Все объекты Пароли Секретные заметки Мои сертификаты Ключи Сег УЛТТЫК КУЭЛАНДЫРУШЫ ОРТАЛЫК (RSA) Промежуточное бюро сертификации Истекает: среда, 25 июня 2025 г. в 10:26:36 Восточный Казахстан, с Оданный сертификат помечен как надежный для этой учетной зап Имя ^ Тип  1270.0.1 Сертификат 127	Связка ключей         ☑         ☑           Все объекты         Пароли         Секретные заметии         Мои сертификаты         Ключи         Сертификат         Сертификат <th>Связка ключей         С сретификаты         С сретификаты         С сретификаты           Все объекты         Пароли         Секретные заметки         Мои сертификаты         Ключи         Сертификаты           УЛТЕЫК КУЭЛАНДЫРУШЫ ОРТАЛЫК (RSA)         Промежуточное бюро сертификации Истекает: среда, 25 июня 2025 г. в 10:26:36 Восточный Казахстан, стандартное время         Срок действия           Имя         Тип         Дата изменения         Срок действия           1220.0.1         Сертификат         сертификат          22 марта 2023 г., 10:15:33           1270.0.1         Сертификат          22 марта 2023 г., 10:26:36           1270.0.1         Сертификат          25 июня 2025 г., 10:26:36           1270.0.1         Сертификат          25 июня 2025 г., 10:26:36           128         ЧПТЪК КУЭЛАНДЫРУШЫ ОРТАЛЫК (RSA)         Сертификат         -         25 июня 2025 г., 10:26:36</th>	Связка ключей         С сретификаты         С сретификаты         С сретификаты           Все объекты         Пароли         Секретные заметки         Мои сертификаты         Ключи         Сертификаты           УЛТЕЫК КУЭЛАНДЫРУШЫ ОРТАЛЫК (RSA)         Промежуточное бюро сертификации Истекает: среда, 25 июня 2025 г. в 10:26:36 Восточный Казахстан, стандартное время         Срок действия           Имя         Тип         Дата изменения         Срок действия           1220.0.1         Сертификат         сертификат          22 марта 2023 г., 10:15:33           1270.0.1         Сертификат          22 марта 2023 г., 10:26:36           1270.0.1         Сертификат          25 июня 2025 г., 10:26:36           1270.0.1         Сертификат          25 июня 2025 г., 10:26:36           128         ЧПТЪК КУЭЛАНДЫРУШЫ ОРТАЛЫК (RSA)         Сертификат         -         25 июня 2025 г., 10:26:36

Рисунок 11. Связка ключей

4. Выберите пункт Доверие:

	ҰЛТТЫҚ КУӘЛАНДЬ	ІРУШЫ ОРТАЛЫҚ (RSA)
	<b>ҰЛТТЫҚ КУӘЛАНДЫР</b> Промежуточное бюро серти Истекает: среда, 25 июня 20 стандартное время З Данный сертификат поме	УШЫ ОРТАЛЫҚ (RSA) іфикации 025 г. в 10:26:36 Восточный Казахстан, ичен для всех пользователей как ненадежный
> Доверие		
🗸 Подробн	lee	
	Тема	
	Страна или регион	KZ
	Общее имя	ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA)
	Кем выдан	
	Общее имя	НЕГІЗГІ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA)
	Организация	РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ»
	Страна или регион	κz
	Серийный номер	35 76 F5 B3 1B 5A 68 21 A1 6F EF AB 12 12 C9 4D 93 8D C7 EE
	Версия	3
	Алгоритм подписи	SHA-256 с шифрованием RSA (1.2.840.113549.1.1.11)
	Параметры	Нет

Рисунок 12. Открытие SSL-сертификата

5. Выберите настройку Параметры использования сертификата и нажмите на Настройки системы:

🔴 🛑 🔹 ҰЛТТЫҚ КУӘЛАНДЫРУ	′ШЫ ОРТАЛЫҚ (RSA)
Сетијеане Макаличка и промежуточное бюро сертифии Истекает: среда, 25 июня 2025 стандартное время З Данный сертификат помечен	Ы ОРТАЛЫҚ (RSA) кации г. в 10:26:36 Восточный Казахстан, для всех пользователей как ненадежный
∨ Доверие	
Параметры использования сертификата:	Настройки системы 🔋 ?
Протокол защищенных сокетов (SSL)	Значение не указано 📀
Безопасная почта (S/MIME)	Значение не указано ᅌ
Расширяемая аутентификация (ЕАР)	Значение не указано ᅌ
IP-безопасность (IPsec)	Значение не указано ᅌ
Подпись кода	Значение не указано ᅌ
Присвоение временных меток	Значение не указано ᅌ
Стандартный алгоритм Х.509	Значение не указано 😌
🗸 Подробнее	
Тема	
<b>Страна или регион</b> KZ	
Общее имя ҰЛ	ТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA)
Кем выдан	

Рисунок 13. Настройка доступов для SSL-сертификата

6. Выберите Всегда доверять и убедитесь, что все пункты изменились:

🔴 🛑 🌒 ҰЛТТЫҚ КУӘЛАНДЫРУ	/ШЫ ОРТАЛЫҚ (RSA)
Сенціване Малини Промежуточное бюро сертифии Истекает: среда, 25 июня 2025 стандартное время З Данный сертификат помечен	<b>Ы ОРТАЛЫҚ (RSA)</b> кации г. в 10:26:36 Восточный Казахстан, г.для всех пользователей как ненадежный
∨ Доверие	
Параметры использования сертификата	/ Настройки системы 🔰 ?
Протокол защищенных сокетов (SSL	Всегда доверять
Безопасная почта (S/MIME	Никогда не доверять
Расширяемая аутентификация (ЕАР)	Значение не указано 📀
IP-безопасность (IPsec)	Значение не указано ᅌ
Подпись кода	Значение не указано ᅌ
Присвоение временных меток	Значение не указано 📀
Стандартный алгоритм Х.509	Значение не указано ᅌ
∨ Подробнее	
Тема	
<b>Страна или регион</b> KZ	
Общее имя ҰЛ	ТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA)
Кем выдан	

Рисунок 14. Добавление SSL-сертификата в доверенные

7. Закройте окно. При необходимости введите пароль администратора для принятия изменений.

Примечание: Если вы используете браузер Mozilla Firefox, то для добавления сертификатов выполните следующие шаги:

1. После установки найдите на рабочем столе три сертификата: 127.0.0.1.cer, nca\_rsa.ctr и root\_rsa.ctr:



2.

				Синхронизация и сохранение данных	Войти
				Новая вкладка	н
				Новое окно	Ħ
				Новое приватное окно	ሪን
				Закладки	
<b>F</b>	irefox			Журнал	
/				Загрузки	f
				Пароли	
				Дополнения и темы	ሪኑ
pec				Печать	ę
				Сохранить как	ţ
				Найти на странице	9
	<b>_</b>		a	Масштаб — 10	0% +
				Настройки	ę
ube	Facebook	Reddit	Amazon		c
				другие инструменты	

Рисунок 16. Открытие меню настроек в браузере Mozilla Firefox

3. Введите в поле поиска Сертификаты и нажмите на Просмотр сертификатов...:

× +	
Firefox about:preferences#searchResults	
	🔍 Сертификаты 🛛 🔇
Результаты поиска	
Сертификаты Запрашивать у OCSP-серверов подтверждение текущего статуса сертификатов	сертификаты Просмотр сертификатов
	Устройства защиты

Рисунок 17. Поиск настроек сертификатов

4. На вкладке Центры сертификации нажмите на кнопку Импортировать:

Ваши сертифик	аты Решения по а	утентификации	Люди	Серверы	Центры сертификации	
∕ вас хранятся <mark>сертиф</mark> и	<mark>икаты</mark> , служащие для иде	нтификации следун	ощих центров	в сертификации		
Имя сертификата		У	стройство за	циты		
$\sim$ AC Camerfirma S.A.						
Chambers of Com	merce Root - 2008	Bui	iltin Object Tol	ken		
Global Chambersign Root - 2008		Bui	iltin Object Tol	ken		
✓ AC Camerfirma SA C	IF A82743287					
Camerfirma Cham	bers of Commerce Root	Bui	iltin Object Tol	ken		
Camerfirma Globa	I Chambersign Root	Bui	iltin Object Tol	ken		
			_			
Просмотреть	Изменить доверие	Импортироват	ть Экс	портировать	Удалить или не доверяти	ь

Рисунок 18. Импорт сертификатов

5. Выберите в окне сертификат nca\_rsa и нажмите кнопку Открыть. Повторите действия для root\_rsa.ctr.

r Избранное (2) Недавние	< > III v III v	📄 Рабочий стол	٢	<b>Q</b> Поиск
🙏 Программы	127.0.0.1.cer			
📃 Рабочий стол		· · · · ·		
Documents			Bartil	Geo
🕑 Загрузки	nca_rsa.crt		Cleruge	dean
Места	root_rsa.crt		Sama	Sm2
iCloud Drive		>		2 3
Теги				
• Красный		>		
😑 Оранжевый		nca, rsa crt		
😑 Желтый		сертификат — 2 К	Б	
• Зеленый		Информация		
• Синий		Создан	E	Вторник, 14 июня 2022 г. в 09:20
• Лиловый	Параметры		C	Отменить Открыть
Солый				

Рисунок 19. Выбор сертификатов для импорта

6. Импорт сертификатов завершен.

# 6 Просмотр устройства хранения ключей и сертификатов пользователя

Для просмотра устройства хранения ключей и сертификатов пользователя выполните следующие действия:

- 1. Вставьте устройство хранения ключевой информации в USB-порт компьютера.
- 2.
- Нажмите на значок Finder 🔛 в Dock, затем дважды щелкните на значок TUMAR\_CSP.



Рисунок 20. Finder. Поиск ПО «ТУМАР-CSP»

3. В окне конфигуратора нажмите на кнопку Настроить ключ.

	Tuma	r CSP Configurator		
Tumar CSP Conf	igurator			ючи недоступны 😣
Лицензи	я выдана HALYK BAN	ik		
<b>HALYK</b>			O moorpa	мме Справка
	Список активны.	х ключевых профайлов		оправка
Настроить ключ	№ Имя профайла	Устройство х	кранения Па	роль
Нажмите чтобы начать работу				
Что-то не работает?				
Нажмите если у вас не	🔍 Список ключей			
holy lactor had points follow	№ Дата создания	Тип данных	Статус ключа	Серийный номер
Выход	Выберите профайл чтобі	ы отобразить ключи Из	менить профайл	Удалить профайл

Рисунок 21. ПО «ТУМАР-CSP». Настройка профайла

- 4. Введите в поле Имя профайла слово token.
- 5. Выберете в списке Устройства хранения выберите тип вашего токена.

	Создание профайла				
Строка профайла:	file:\\user				
Имя профайла:	token				
Устройство хранения:	√ file				
Параметры устройства хранения:	javatoken kztoken newoids				
Пароль:					
Повторить пароль:					
Формат ключевого контейнера:					
Tumar (.bin)	Tumar (.pem)				
Имя контейнера:	Users				
	Сохранить Отмена				

Рисунок 22. ПО «ТУМАР-CSP». Выбор устройства хранения

6. Выберете в списке Параметры устройства хранения доступное значение.

	Создание профаил	la	
Строка профайла:	file:\\user		
Имя профайла:	token		
Устройство хранения:	newoids		
Параметры устройства хранения:	SafeNet eToken 5100		Обзор
Пароль:	SafeNet eToken 5100		
Повторить пароль:			
Формат ключевого конте	ейнера:		
Имя контейнера:	Users		
		Сохранить	Отмена

Рисунок 23. ПО «ТУМАР-CSP». Выбор параметра устройства хранения

**Важное замечание:** Название зависит от используемого устройства хранения ключевой информации и может отличаться от приведенного в примере.

#### 7. Нажмите на кнопку Сохранить.

8. Убедитесь, что в созданном профайле отображаются ключи и сертификаты, находящиеся на устройстве хранения ключевой информации.

		Tumar C	SP Configurator		
Tumar CSP Confi	igura	ator		Дост	упно ключей (8) 🖌
Лицензия	і выда	на HALYK BANK			
				О програм	име Справка
		Список активных кл	пючевых профайлов		
Настроить ключ	N⁰	Имя профайла	Устройство хра	нения Пар	ооль
Нажмите чтобы начать работу	1	🔨 token	newoids	1	YES
Что-то не работает? Нажмите если у вас не	•	O			
получается настроить ключ	-		<b>T</b>	0	0
	Nº	дата создания	Гип данных	Статус ключа	Серииный номер
	1	2023.12.27 03.12.41	Сертификат и ключ	Просрочен: 20 д	Oe d2 fd 64 7d e5 e4 eb 69
	2	2023.01.18 03:24:14	Сертификат и ключ	Осталось 1 дней	45 d1 4b 25 aa b4 d8 26 2d
	4	2023.08.03 05:04:19	Ключ и цепочка серти	Осталось 198 дн	36 11 12 1f 61 13 28 da bb
	5	2023.08.03 05:20:	Ключ и цепочка сер	Осталось 198 д	67 2f 0c 4c aa 1f 46 1b 98 1
Выход	Выбер	ите профайл чтобы от	образить ключи Изме	енить профайл	Удалить профайл

Рисунок 24. ПО «ТУМАР-CSP». Настройка профайла завершена успешно

9. Проверка устройства хранения ключевой информации завершена.

## 7 Список плагинов поддерживаемых в CryptoSocket

Для просмотра списка поддерживаемых плагинов CryptoSocket:

- 1. Нажмите правой кнопкой мыши на значок CryptoSocket в системном трее.
- 2. Выберите пункт меню Плагины.



Рисунок 25. Список плагинов

## 8 Выход из CryptoSocket

Для завершения работы CryptoSocket:

- 1. Нажмите правой кнопкой мыши на значок CryptoSocket в системном трее.
- 2. Выберите пункт меню Выход.



Рисунок 26. Выход из CryptoSocket