

«Signal-COM AuthKey»

одноключевая

усиленная неквалифицированная электронная подпись

Разработанное АО "Сигнал-КОМ" инновационное решение для создания одноключевой усиленной неквалифицированной электронной подписи (НЭП) обеспечивает высокий уровень безопасности и юридической значимости электронных документов, соответствуя всем современным требованиям.

«Signal-COM AuthKey» — это надежный инструмент для защиты информации, который позволяет определить подписанта и обнаружить любые изменения в документе после его подписания. Это делает его идеальным для использования в различных информационных системах, где требуется подтверждение подлинности и целостности данных.



Алгоритмы и СКЗИ

Одноключевая усиленная НЭП реализована по алгоритмам HMAC_GOSTR3411_2012_256 и HMAC_GOSTR3411_2012_512, в соответствии с RFC 2104 (HMAC: Keyed-Hashing for Message Authentication) и Рекомендациям по стандартизации Р 50.1.113-2016 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования».

Решение построено на базе СКЗИ «Signal-COM JCP 3.1» (варианты исполнения 1, 2), сертифицированных ФСБ России (Сертификаты СФ/114-4344, СФ/124-4345 от 18 сентября 2022 г.), что подтверждает соответствие высоким стандартам безопасности и надежности.



HMAC_GOSTR3411_2012_256

Алгоритм для
криптографической защиты.



HMAC_GOSTR3411_2012_512

Усиленный алгоритм для
большей безопасности.



Сертификация ФСБ России

СКЗИ «Signal-COM JCP 3.1» сертифицированы ФСБ России.

Нормативная база

**ФЗ от 06.04.2011
№ 63-ФЗ
«ОБ ЭЛЕКТРОННОЙ ПОДПИСИ»**

Определяет НЭП как подпись,
созданную с использованием ключа,
позволяющую определить
подписанта и обнаружить
изменения.

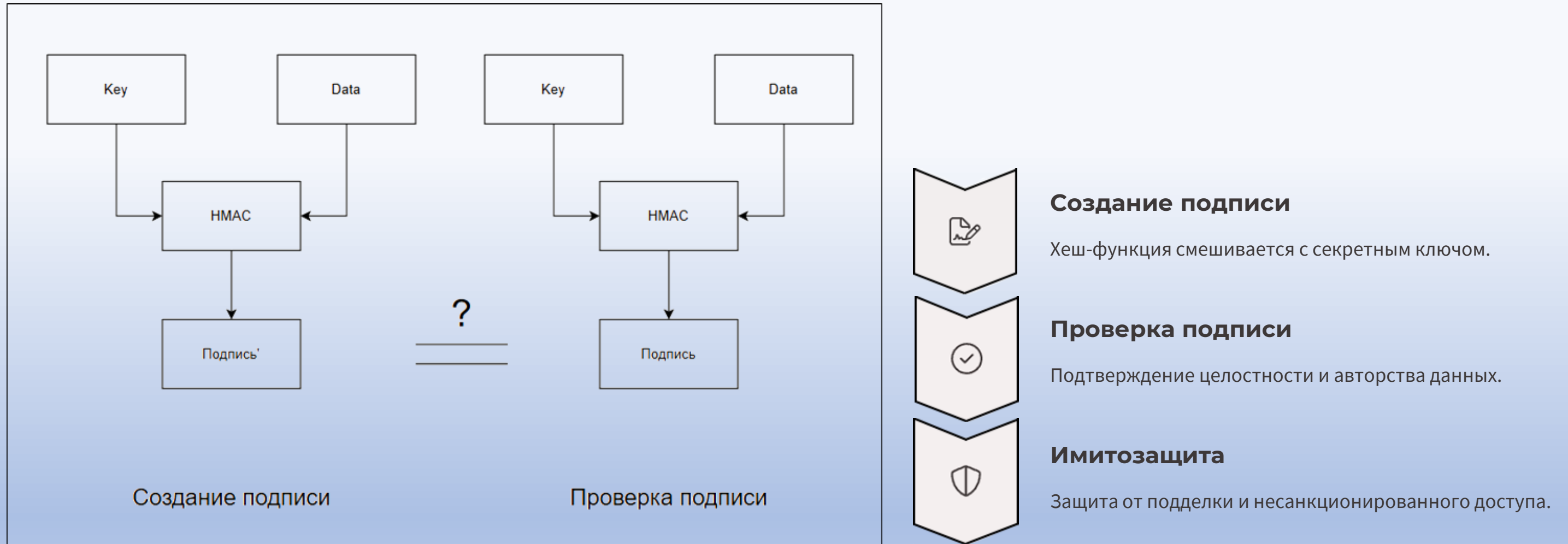
**Положение Банка России
от 17.04.2019
№ 683-П
(подпункт 5.1 пункта 5)**

Требует обеспечения целостности
электронных сообщений и
подтверждения авторства.

**Положения
информационного письма
Банка России
от 16.03.2023 № ИН-017-56/22**

Допускает использование
усиленной НЭП и СКЗИ для
указанных целей.

Создание и проверка усиленной НЭП



Процесс создания и проверки усиленной НЭП в «Signal-COM AuthKey» разработан для максимальной простоты и надежности. Пользователи могут легко генерировать ключи, формировать подписи и проверять их подлинность, обеспечивая полноценную безопасность своих данных.

Сравнение одноключевой и двухключевой ЭП

Одноключевая и двухключевая электронные подписи имеют свои особенности применения. Двухключевая ЭП обеспечивает более широкое применение, но требует развертывания Инфраструктуры Открытых Ключей (PKI) с использованием Удостоверяющего Центра, что значительно повышает стоимость ее использования.

Одноключевая ЭП в архитектуре ИС типа "звезда" не уступает двухключевой, но намного проще в реализации и значительно ниже по стоимости. Использование одноключевой ЭП в "облаке" упрощает работу и не требует доработки существующего клиентского ПО.

	Одноключевая ЭП	Двухключевая ЭП
Архитектура ИС "каждый с каждым"	-	+
Архитектура ИС "звезда"	+	+
Наличие ИОК (PKI)	Не требуется	Требуется
Типы поддерживаемых ЭП: КЭП	-	+
Типы поддерживаемых ЭП: НЭП	+	+
Сертификация СКЗИ	+	+

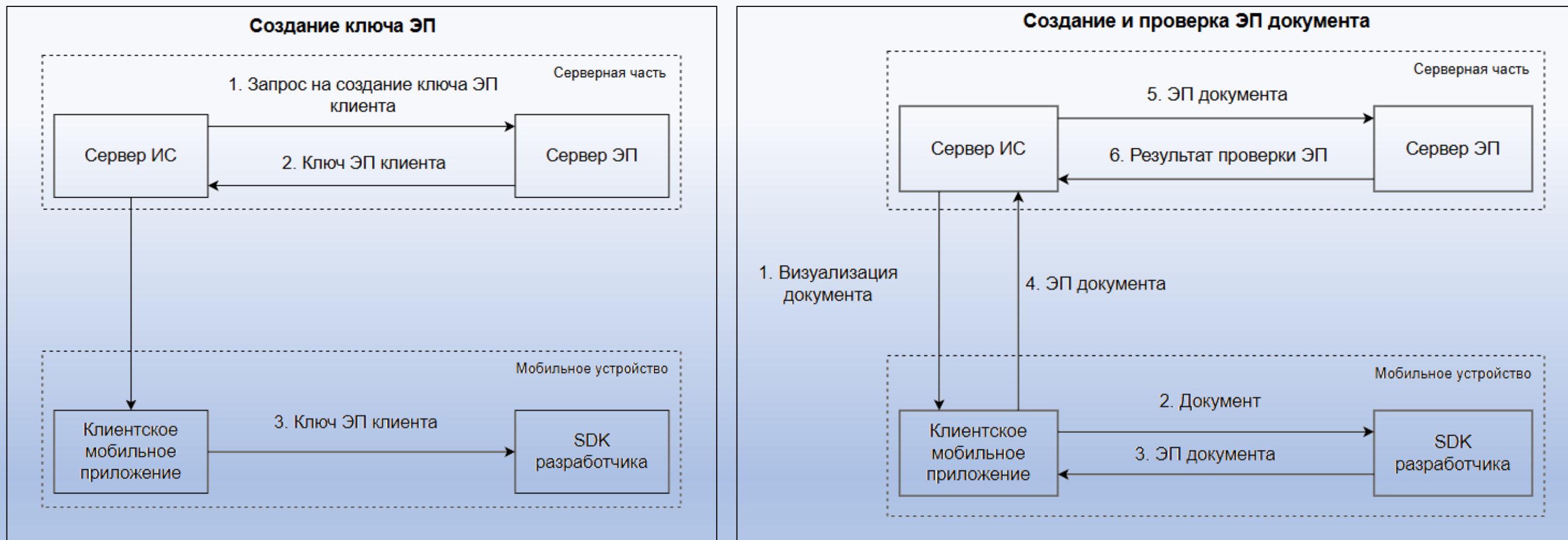
Варианты поставки

Первый вариант — формирование НЭП на клиенте с проверкой на сервере, что идеально подходит для мобильных приложений (Android, iOS) с использованием «Signal-COM AuthKey SDK».

Второй вариант — формирование и проверка НЭП на сервере (дистанционное облачное решение), которое не требует доработки клиентских приложений. Обеспечивает максимальное удобство и быструю интеграцию в существующие системы.

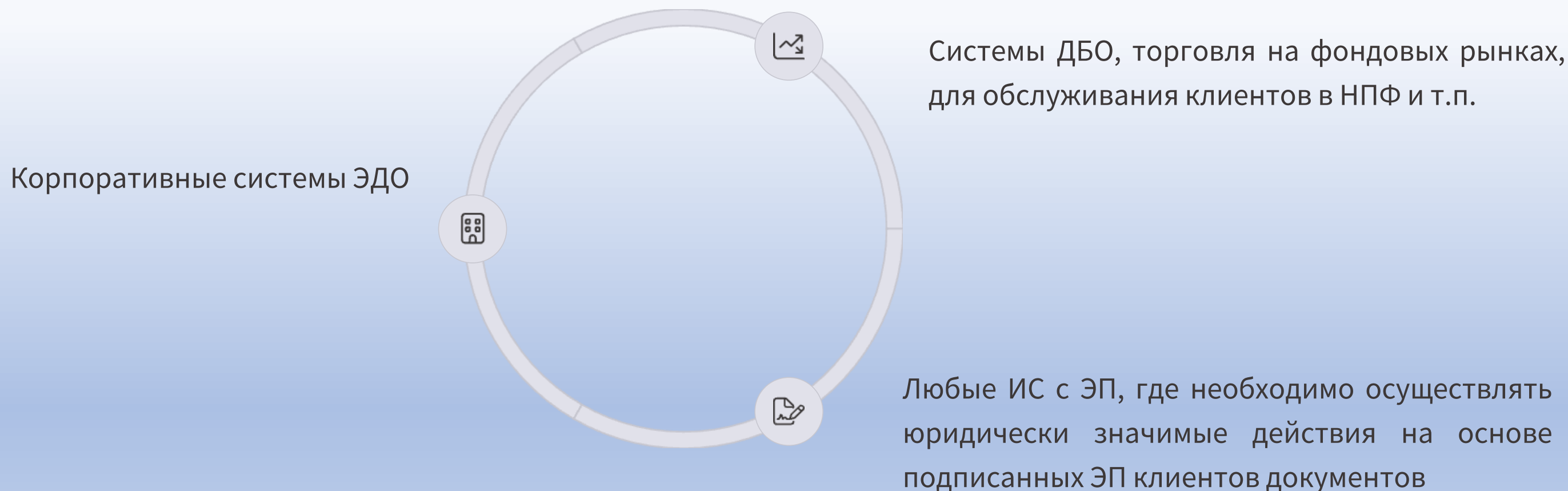


Генерация ключей, формирование и проверка НЭП в «Signal-COM Authkey». Структурная схема.



Сферы применения

Внедрение «Signal-COM AuthKey» не требует высоких затрат и может быть использовано в широком спектре информационных систем. Это универсальное решение для обеспечения юридической значимости электронных документов и действий клиентов.



Вопросы?



Сигнал-КОМ

Криптографическая защита информации

Адрес офиса:



Россия, г. Москва, ул. Ленинская Слобода, д.19,
строение. 3, этаж 3



signal@signal-com.ru

Телефоны:



+7 (495) 969-30-34 (Секретарь)



+7 (495) 363-30-73 (Отдел продаж)



+7 (495) 363-30-93 (УЦ и техподдержка)



+7 (926) 779-68-16 (Экстренная связь)

Если у вас возникли вопросы или вы хотите узнать больше о «Signal-COM AuthKey», пожалуйста, свяжитесь с нами. Наша команда готова предоставить всю необходимую информацию и поддержку.