

Крипто-ключ для ЕГАИС

Регистрационный номер из 1С – ТЗ_ОТС_103/25 от 23.09.2025

Срок действия: 1 год.

Функциональное предназначение: Аппаратный крипто-ключ для проверки, формирования и безопасного хранения ключей электронной подписи и ключей шифрования, поддерживающих работу в ЕГАИС.

Объекты, на которых используется оборудование:

Магазин Магнит	Да
Магнит Косметик	Нет
Магнит Аптека	Нет
Гипермаркет	Да
Магнит Опт	Да
Распределительный центр	Да
Автотранспортное предприятие	Нет
Офисы	Нет

Требования (минимальные):

1. Общие параметры:
1.1. Сертификация производства (Россия)
1.2. Сертификация изделия (Россия)
2. Минимальные технические параметры:
2.1. Форм-фактор — компактный носитель информации, содержащий в себе защищенный микропроцессор и операционную систему, контролирующую устройство, доступ к оперативной и долговременной памяти.
2.2. Выполнение всех необходимых криптографических операций внутри устройства без использования внешних криптографических ресурсов.
2.3. Аппаратная реализация стандартов электронной подписи, шифрования и хеширования с использованием криптографических стандартов ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2015/ГОСТ 34.12-2018, ГОСТ Р 34.13-2015/ГОСТ 34.13-2018 (Кузнечик и Магма).
2.4. Защита закрытых ключей от копирования во внешнюю вычислительную систему.
2.5. Защита оперативной и долговременной памяти от копирования и несанкционированного доступа.
2.6. Использование одновременно без ограничений российских и зарубежных криптоалгоритмов.
2.7. Соответствие требованиям Федерального закона от 06.04.2011 N 63-ФЗ "Об электронной подписи" для создания усиленной квалифицированной электронной подписи.
2.8. Реализация криптоалгоритмов:
2.8.1. AES (длины ключей 128, 192, 256 бит);
2.8.2. 3DES (длины ключей 168 бит);
2.8.3. RSA (длины 1024, 2048);
2.8.4. криптография на эллиптических кривых (длины ключей 512 бит) (ГОСТ);
2.8.5. западная криптография на эллиптических кривых (аппаратная реализация);

2.8.6.	аппаратная генерация ключей для RSA и криптографии на эллиптических кривых (ГОСТ);
2.8.7.	аппаратная генерация случайных чисел;
2.8.8.	алгоритмы согласования ключей: алгоритм Диффи-Хеллмана, алгоритм Диффи-Хеллмана на эллиптических кривых;
2.8.9.	функции хэширования: SHA-1, SHA-256 (аппаратная реализация);
2.8.10.	ГОСТ Р 34.10-2012 (генерация ключевых пар, формирование и проверка электронной подписи);
2.8.11.	ГОСТ Р 34.11-2012 (функция хэширования);
2.9.	Взаимодействие через библиотеку связи, реализующую стандарт PKCS-11 (включая ГОСТ Р 34.10-2012). Библиотека должна поддерживать работу на оборудовании со следующими операционными системами:
2.9.1.	Windows 10 (32/64-бит)
2.9.2.	Windows 11 (64-бит)
2.9.3.	Windows Server 2022
2.9.4.	Windows Server 2019
2.9.5.	Windows Server 2016
2.9.6.	Rocky Linux 9
2.9.7.	Oracle Linux 8
2.9.8.	CentOS 6, 7 (32/64-бит)
2.9.9.	Debian 12 x32_64
2.10.	Обеспечение работы крипто-ключа в актуальной версии программного обеспечения УТМ автоматизированной системы, предназначенной для государственного контроля за объемом производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции (ЕГАИС) под управлением операционных систем:
2.10.1.	Windows 10 (32/64-бит)
2.10.2.	Windows 11 (64-бит)
2.10.3.	Windows Server 2022
2.10.4.	Windows Server 2019
2.10.5.	Windows Server 2016
2.10.6.	Rocky Linux 9
2.10.7.	Oracle Linux 8
2.10.8.	CentOS 6, 7 (32/64-бит)
2.10.9.	Debian 12 x32_64
2.11.	Обеспечение функциональности неубывающего счетчика. Каждая электронная подпись, успешно рассчитанная крипто-ключом, должна обеспечивать увеличение значения счетчика на единицу. Встроенное программное обеспечение аппаратного крипто-ключа не должно содержать открытых программных интерфейсов, с помощью которых можно изменить значение счетчика. Счетчик не должен терять свое значение при переформатировании аппаратного крипто-ключа. Выдаваемое значение счетчика должно сопровождаться криптографической контрольной суммой.
2.12.	Криптографическая контрольная сумма должна представлять собой результат расчета электронной подписи от следующих параметров:
2.12.1.	Аппаратный номер карты
2.12.2.	Значение дайджеста последних данных, от которых рассчитывалась электронная подпись
2.12.3.	Значение счетчика
2.13.	Значение электронной подписи должно вычисляться с использованием специальной ключевой пары. Пара должна содержать сигнальный атрибут и / или иные средства, препятствующие использованию этой пары в других процедурах подписания помимо расчета контрольной суммы.
2.14.	Операции инициализации области ключа или форматирования, генерации ключевой пары не должны превышать более 1 мин.

2.15.	Максимальная длина пин-кодов пользователя и администратора для всех программных областей крипто-ключа должна быть не менее 12 символов.
2.16.	Комплект сопроводительной документации к каждой партии криптоключей должен в себя включать в бумажном варианте:
2.16.1.	Правила пользования СКЗИ;
2.16.2.	Формуляр, включающий в себя копию сертификата ФСБ, список серийных номеров (ID) криптоключей и десятичные номера ФСБ.
2.17.	Срок гарантийного обслуживания — не менее 3 лет.
2.18.	Срок диагностики — не более 3-х рабочих дней.
2.19.	Срок гарантийного обмена — не более 30 календарных дней
2.20.	Требование замены по гарантии – отправка в СЦ и возврат за счет поставщика, силами курьерской службы с филиалов Компании. Забор осуществляется на основании акта-рекламации. Поставщик не вправе возвращать денежные средства или их эквивалент взамен неисправных криптоключей, по которым подтвержден гарантийный случай, только новые, исправные криптоключи, соответствующие данному Техническому Заданию.
2.21.	Требования к оказанию технической поддержки по эксплуатации крипто-ключа:
2.21.1.	Гарантированный ответ (консультация) по телефону и по электронной почте.
2.21.2.	Консультирование по вопросам эксплуатации крипто-ключа
2.21.3.	Максимальный срок реакции на запрос технической поддержки не более 4 часов
2.21.4.	Наличие сервиса для проведения диагностики крипто-ключа
2.21.5.	Режим оказания технической поддержки 24x7
2.21.6.	Язык технической поддержки русский
2.21.7.	Способ приема запросов на техническую поддержку Телефон, E-Mail.

Ответственные за согласование:

Подразделение	Ф.И.О.	Пункты для согласования
Департамент сопровождения ИТ Управление по ИТ-сопровождению регионов	Шаранов Д.С.	2.17, 2.20, 2.21.7
Департамент инфраструктуры и защиты информации Отдел информационной безопасности	Дордий М.А.	Все
Департамент сопровождения ИТ Управление по сопровождению продаж	Ростовский-Сериков К.С.	2.9, 2.10
Департамент по развитию и разработке ИС цепочек поставок и складской логистики Направление сопровождения логистики	Беляева И. В.	2.9, 2.10
Департамент по некоммерческим закупкам Отдел сопровождения категории ИТ оборудование/ПО и персонала	Власюк И. А.	Все