ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ
по приобретению носителей ключевой информации Удостоверяющего центра государственных органов

Наименование	Требование
Общие требования	Потенциальный поставщик, должен предоставить протокол тестирования работы устройства хранения ключевой информации с криптопровайдером Tumar CSP 6.3 (совместно с поставщиком средств криптографической защиты информации УЦ ГО), подтверждающий корректность работы устройства с TumarCSP 6.3.

Наименование	Технические характеристики	
носители ключевой информации для УЦ ГО USB	Объем защищенной памяти	Не менее 64 КБ памяти
	Форм факторы носителя ключевой информации	USB-ключ
	Поддерживаемые ОС	Windows 2000/2003/2008/2012 Server/ XP /Vista/7/8/10 Linux и т.д.
	Совместимость со средствами криптографической защиты информации	Tumar CSP V6.3.
	Поддерживаемые интерфейсы и стандарты	PKCS#11: v2.01, Microsoft CryptoAPI, X.509 v3 certificate storage, SSL v3.6
	Аппаратно реализованные алгоритмы	ГОСТ 34.310-2004, ГОСТ 34.311-95, СТ РК ГОСТ Р 34.10-2015
	Генерация ключей ГОСТ 34.310-2004	Не более 15 сек
	Время формирования ЭЦП (размер файла 60 Мб)	Не более 10 сек.
	Световой индикатор режимов работы	On / Off / мигает
	Тактовая частота процессора	Не менее 6 МГц
	Поддержка Reset и "спящего" режима USB (Suspend mode)	Да
	Потребляемая мощность	Меньше 250 мВт
	Интерфейс / Разъем	USB 2.0, 3.0
	Размеры	Не более 80 х 20 х 15 мм
	Корпус	Твердый пластик
	Серийный номер	Наличие уникального серийного номера на корпусе носителя ключевой информации
	Вес	Не более 50 г
	Среднее время наработки на отказ электронных компонентов	Не менее 10 лет
	Срок хранения данных в памяти	Не менее 10 лет
	Количество циклов перезаписи памяти	Не менее 500 000 раз
	Сертификация	Соответствие требованиям 3 (третьего) уровня безопасности СТ РК 1073-2007, с отсутствием

		возможности выпускать регистрационное свидетельство по требованиям 2(второго) уровня безопасности СТ РК 1073-2007.
	Гарантийный срок	1 год
	Генерация ключей ГОСТ 34.310-2004, СТ РК ГОСТ Р 34.10-2015	Возможность генерации ключей на устройстве и отсутствие возможности экспорта закрытого ключа с устройства

Мемлекеттік органдар куаландіру орталығына арналған кілтті ақпаратты тасығыш сатып алу
ТЕХНИКАЛЫҚ ЕРЕКШЕЛІГІ

Атауы	Талаптар
Жалпы талаптар	Әлеуетті өнім беруші құрылғының Tumar CSP V6.3. криптопровайдері бар кілтті ақпаратты сақтау құрылғысының жұмысын тестілеу (МО КО-ның ақпаратты криптографиялық қорғау құралдарын жеткізушімен бірлесіп) хаттамасын ұсынуға тиіс.

Атауы	Техникалық ерекшеліктер	
МО КО-ға арналған кілтті ақпаратты тасығыш USB	Қорғалған жадының көлемі	Жадының 64 КБ кем емес
	Кілтті ақпараттық тасығыш форм факторлары	USB-кілт
	Қолдау көрсетілетін ОЖ-лар	Windows 2000/2003/2008/2012 Server/ XP /Vista/7/8/10 Linux
	Ақпараттық криптографиялық қорғау құралдарымен үйлесімділік	Tumar CSP V6.3.
	Қолдау көрсетілетін интерфейстер мен стандарттар	PKCS#11: v2.01, Microsoft CryptoAPI, X.509 v3 certificate storage, SSL v3.6
	Ақпараттық іске асырылған алгоритмдер	МЕМСТ 34.310-2004, МЕМСТ 34.311-95, ҚР СТ. МЕМСТ Р 34.10-2015
	МЕМСТ 34.310-2004 кілттерін шығару	15 сек. кем емес
	ЭЦҚ-ны қалыптастыру уақыты (файла өлшемі 60 Мб)	10 сек. кем емес
	Жұмыс режимдерінің жарық индикаторы Световой индикатор режимов работы	On / Off / жыпылықтайды
	Процессордың тактілік жиілігі	6 МГц кем емес
	Reset және USB (Suspend mode) "ұйқы" режимін қолдау	Иә

	Тұтынатын қуаты	250 мВт кем
	Интерфейсі / Ажыратқыш	USB 2.0, 3.0
	Өлшемдері	80 х 20 х 15 мм артық емес
	Корпусы	Қатты пластик
	Сериялық нөмірі	Кілтті ақпаратты тасығыштың корпусында бірегей сериялық нөмірі болуы
	Салмағы	50 г. артық емес
	Электрондық компонеттерінің істен шыққанға дейінгі орташа жұмыс істеу уақыты	10 жылдан кем емес
	Деректерді жадыда сақтау мерзімі	10 жылдан кем емес
	Жадыны қайта жазу кезеңдерінің саны	500 000 реттен кем емес
	Сертификаттау	ҚР СТ 1073-2007 бойынша 3 үшінші қауіпсіздік деңгейі талаптарына сәйкестік, ҚР СТ 1073-2007 қауіпсіздіктің 2(екінші) деңгейінің талаптарына сәйкес тіркеу куәлігін шығару мүмкіндігі жоқ.
	Кепілдік мерзімі	1 жыл
	МЕМСТ 34.310-2004, ҚР СТ. МЕМСТ 34.10-2015кілттерін шығару	Құрылғыда кілттерді генерациялау мүмкіндігі және құрылғыдан Жабық кілтті экспорттау мүмкіндігінің болмауы