

Формат журнала Рутокен ЭЦП

Журнал операции Рутокен ЭЦП представляет собой TLV-структуру 0x80, в поле V которой находится набор следующих TLV-структур в произвольном порядке.

Значение в поле Tag (T)	Значение в поле Length (L)	Содержимое поля Value (V)
0xAA	Размер хэша в байтах	Хэш от подписываемых данных
0xB6	Размер электронной подписи хэша в байтах	Электронная подпись хэша
0x85	12	Информация о выполненной операции: • Тип операции (в текущей версии поддерживается только 0x1 – операция подписи) – 1 байт; • Тип ключа, на котором была выполнена операция – 1 байт; • Флаги предназначения ключа, на котором была выполнена операция – 1 байт; • Флаги выполнения операции – 1 байт; • Резерв (должен содержать 0) – 1 байт; • Резерв (должен содержать 0) – 1 байт; • Системный идентификатор ключа, на котором была выполнена операция – 2 байта, big-endian. • Текущее значение общего счетчика удачных операций подписи – 4 байта, big-endian.
0x83	8	Уникальный идентификатор устройства Рутокен, big-endian

Типы ключей

В текущей версии Рутокен ЭЦП поддерживаются следующие типы ключей.

B7	B6	B5	B4	B3	B2	B1	B0	Тип ключа
0	0	0	0	0	0	1	1	закрытый ключ ГОСТ Р 34.10–2001
0	0	1	0	0	0	1	1	закрытый ключ RSA
0	1	0	0	0	0	1	1	закрытый ключ ГОСТ Р 34.10–2012
0	0	0	1	0	0	1	1	открытый ключ ГОСТ Р 34.10–2001
0	0	1	1	0	0	1	1	открытый ключ RSA
0	1	0	1	0	0	1	1	открытый ключ ГОСТ Р 34.10–2012

Флаги предназначения ключей

В текущей версии Рутокен ЭЦП поддерживаются следующие флаги предназначения ключей.

B7	B6	B5	B4	B3	B2	B1	B0	Флаги предназначения ключа
						X	X	Флаги предназначения ключа:
						0	X	1 – для электронной подписи и обмена ключами 0 – только для электронной подписи
						X	1	1 – для Secure Messaging 0 – для обмена ключами
					0			Зарезервирован (должен содержать '0')
				0				Зарезервирован (должен содержать '0')
			0					Зарезервирован (должен содержать '0')
		0						Зарезервирован (должен содержать '0')
0	0							Зарезервированы (должны содержать '0')

Флаги выполнения операции

В текущей версии Рутокен ЭЦП поддерживаются следующие флаги выполнения операции.

B7	B6	B5	B4	B3	B2	B1	B0	Флаги выполнения операции
							1	Хэш от подписываемых данных был вычислен Рутокен ЭЦП (иначе – хэш был получен извне)
						0		Резерв (имеют значение '0')
			0	0				Резерв (имеют значение '0')
		0						Резерв (имеют значение '0')
		0						Резерв (имеют значение '0')
0	0							Резерв (имеют значение '0')

Общий счетчик удачных операций

Общий счетчик удачных операций подписи имеет следующие свойства:

- Хранится в области структурированных данных, не стирается в процессе пользовательского форматирования;
- Значение счетчика инкрементируется после каждой успешно проведенной операции подписи на ключе ГОСТ.