МИКРОКОНТРОЛЛЕРЫ. ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

	80 Кб (EEPROM)	160 Кб (EEPROM)	320 Кб (flash)	384 Кб (flash)
тип процессорного ядра	8/16 разрядное процессорное ядро		ARMSecureCoreSC000 32-bit RISC	
внутренний тактовый генератор	29 МГц		28 МГц	
RAM (оперативная память)	8 Кбайт		10 Кбайт	12 Кбайт
ROM (масочное ПЗУ)	390 Кбайт		-	-
EEPROM (энергонезависимая память данных)	80 Кбайт	160 Кбайт	320 Кбайт Flash	384 Кбайт Flash
внешний интерфейс	Контактный в соответствии с ISO7816 (протокол T=0,T=1, внешний CLOCK до 10 МГц)	Контактный в соответствии с ISO7816 (протокол T=0,T=1, внешний CLOCK до 10 МГц) Бесконтактный интерфейс в соответствии с ISO14443-B	Контактный в соответствии с ISO7816 (протокол T=0,T=1, внешний CLOCK до 10 МГц)	Контактный в соответствии с ISO7816 (протокол T=0,T=1, внешний CLOCK до 10 МГц) Бесконтактный интерфейс в соответствии с ISO14443-A/B
криптосопроцессор для криптографии с открытым ключом	есть			
встроенный генератор случайных чисел **аппаратные средства защиты от динамического исследования методами SPA, DPA, DFA** **аппаратные средства защиты от статического исследования**	есть			
гарантируемое время хранения данных в энергонезависимой памяти	30 лет			
гарантируемый технический ресурс энергонезависимой памяти	500000 циклов стирания/записи			
сертификация на соответствие ISO15408 Common Criteria	EAL 6+		EAL 5	
сертификация на соответствие требованиям EMVco	есть			
российские криптоалгоритмы	Криптоалгоритмы симметричной криптографии ГОСТ 28147-89 ГОСТ Р 34.12-2015 / ГОСТ 34.12-2018 («Магма») Криптоалгоритмы ЭП ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (256 бит) ХЭШ ГОСТ Р34.11-94 ГОСТ Р34.11-2012 Сертифицированный в ФСБ России по классу КС2 криптомодуль (СКЗИ «Криптомодуль С23», сертификат СФ/114-1511 от 08 июля 2010 г.), (ГОСТ 28147-89, ГОСТ Р34.10-2001); АМ СКЗИ «Форос 2»		Криптоалгоритм симметричной криптографии ГОСТ 28147-89 ГОСТ Р34.12-2015 («Магма» и «Кузнечик» / ГОСТ 34.12-2018) ГОСТ Р34.13-2015/ГОСТ 34.13-2015 Криптоалгоритм ЭП ГОСТ Р34.10-2012 (256 и 512 бит) / ГОСТ 34.10-2018 ХЭШ ГОСТ Р 34.11-94 ГОСТ Р34.11-2012 (256 и 512 бит) / ГОСТ 34.11-2018 HMAC_GOSTR3411_2012_256, HMAC_GOSTR3411_2012_512 в соответствии с Р 50.1.113-2016 VKO_GOSTR3410_2012_256, VKO_GOSTR3410_2012_512 в соответствии с Р 50.1.113-2016 VKO GOST R 34.10-2001 в соответствии с RFC 4357 KDF_GOSTR3411_2012_256 и KDF_GOSTR3411_2012_512 в соответствии с RFC7836	
международные криптоалгоритмы	DES / 3DES, RSA, ХЭШ-функция SHA-1		RSA, ECDSA, DES, 3DES, SHA-1, SHA-256	
сертификация ФСБ России	КС1, КС2		КС1, КС2, КС3	
сертификация ФСТЭК России	УД4			
операционная система	ОС «Магистра 1.30»		СКЗИ ОС «ФОРОС 2.01»	