РусКрипто

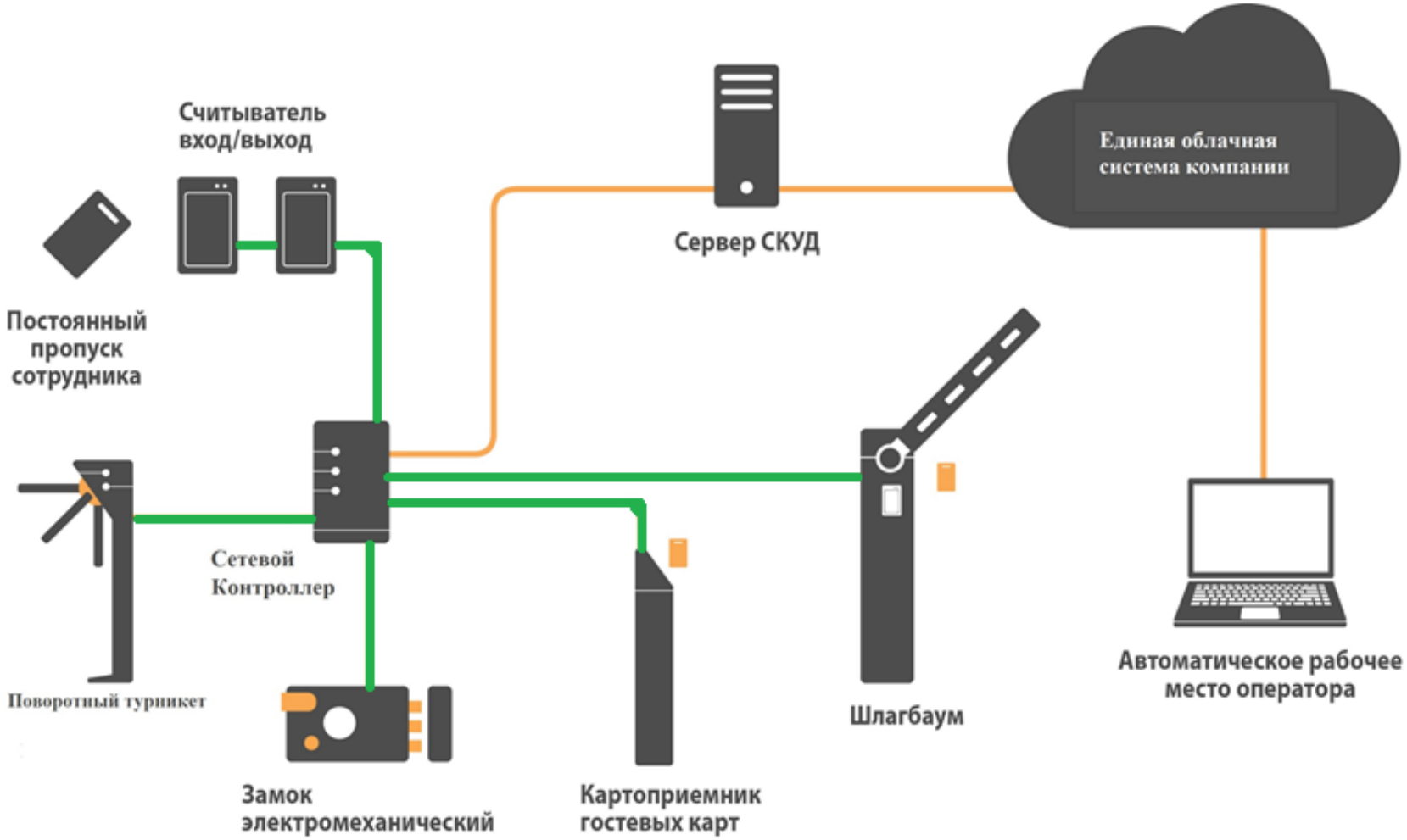
КОМПАНИЯ АКТИВ

Модификация протокола OSDP для СКУД с использованием российских криптоалгоритмов

Максим Архипов

Компания «Актив»

Общая схема СКУД



Актуальность проблемы

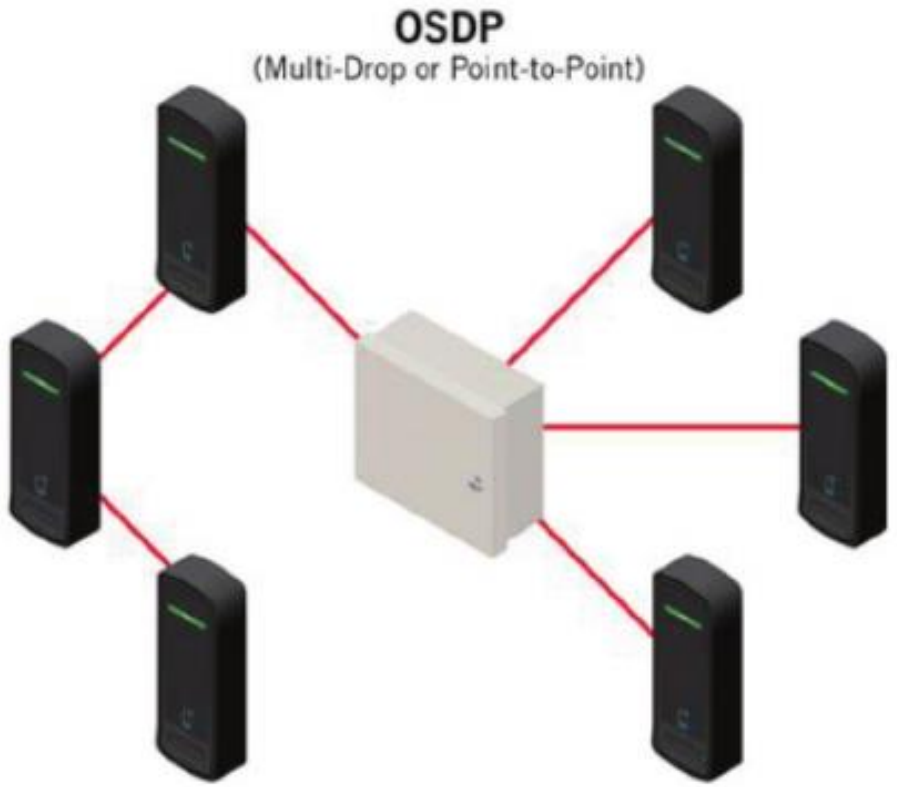
- Устаревшие решения
- Отсутствие стандарта
- Зависимость от зарубежных технологий

Цель проекта:

Адаптировать OSDP под российские криптостандарты, сохранив функциональность и совместимость с существующими системами

OSDP

- Безопасность
- Двухсторонняя связь
- Гибкость и масштабируемость
- Стандартизация Международной электротехнической комиссией IEC 60839-11-5



Формат пакетов

Данные пакета

Заголовок пакета

Опционально

Обозначение байтов	Описание
SOM	Начало сообщения
ADDR	Адрес считывателя
LEN_LSB, LEN_MSB	Длина пакета
CTRL	Наличие security block
SEC_BLK_LEN	Длина security control block
SEC_BLK_TYPE	Тип security block
SEC_BLK_DATA	Данные security block
CMND/REPLY	Код команды или ответа
DATA	Данные пакета
MAC	4 первых байта MAC сообщения
CKSUM/CRC_LSB	Контрольная сумма

Команды, принимаемые считывателем

Команда	Описание
osdp_POLL	Опрос
osdp_ID	Запрос получения id
osdp_CAP	Запрос возможностей устройства
osdp_LSTAT	Запрос отчета о состоянии
osdp_LED	Управление светодиодом
osdp_BUZ	Управление звонком считывателя
osdp_SCRYPT	Криптограмма контроллера
osdp_KEYSET	Команда установки ключа шифрования
osdp_CHLNG	Инициализация защищенного канала

Ответы, отправленные считывателем

Команда	Описание
osdp_ACK	Команда принята
osdp_NAK	Команда не обработана
osdp_PDID	ID считывателя
osdp_PDCAP	Отчет о возможностях устройства
osdp_LSTATR	Отчет о состоянии
osdp_RAW	Данные карты
osdp_KPD	Данные клавиатуры
osdp_COM	Скорость передачи данных
osdp_CCRYPT	ID считывателя, случайное число, криптограмма считывателя
osdp_RMAC_I	Инициализация R-MAC

Базовый ключ

- В контроллер предварительно зашивается Master key.
- Контроллер с помощью команды osdp_KEYSET передает Master key считывателю

$$SCBK = E_{masterkey}(cUID || \sim cUID)\ ,$$

где cUID – серийный номер считывателя,
~cUID – побитовая инверсия cUID

Схема защищенного канала

Контроллер $[SCBK]$		**Считыватель** $[SCBK]$
$RND_A \xleftarrow{\mathcal{U}} \{0,1\}^{rlen}$	$\xrightarrow{RND_A}$	$RND_B \xleftarrow{\mathcal{U}} \{0,1\}^{rlen}$
		$K_{enc} \leftarrow \mathsf{E}_{SCBK}(C_1 \parallel RND_A \parallel C_0)$ $K^1_{mac} \leftarrow \mathsf{E}_{SCBK}(C_2 \parallel RND_A \parallel C_0)$ $K^2_{mac} \leftarrow \mathsf{E}_{SCBK}(C_3 \parallel RND_A \parallel C_0)$
выработать $K_{enc}, K^1_{mac}, K^2_{mac}$	$\xleftarrow{RND_B, Crypto_{AB}}$	$Crypto_{AB} \leftarrow \mathsf{E}_{K_{enc}}(RND_A \parallel RND_B)$
проверить корректность		
$Crypto_{BA} \leftarrow \mathsf{E}_{K_{enc}}(RND_B \parallel RND_A)$	$\xrightarrow{Crypto_{BA}}$	проверить корректность
	$\xleftarrow{IV_A}$	$IV_A \leftarrow \mathsf{E}_{K^2_{mac}}\left(\mathsf{E}_{K^1_{mac}}(Crypto_{BA})\right)$

..... Процедура установки ключей завершена .....

C_0, C_1, C_2, C_3 — константы

Шифрование пакетов

$ct_A \leftarrow \mathsf{CBC}_{K_{enc}}^{IV_A}(m_A)$

$\tau_A \leftarrow \mathsf{CBCMAC}_{K^1_{mac},K^2_{mac}}^{IV_A}(ad_A \parallel ct_A)$

$IV_B \leftarrow \tau_A$

$ad_A \parallel ct_A \parallel \tau_A[0:3] \longrightarrow$

проверка τ_A

расшифровка ct_A

$IV_B \leftarrow \tau_A$

$ct_B \leftarrow \mathsf{CBC}_{K_{enc}}^{IV_B}(m_B)$

проверка τ_B

$\longleftarrow ad_B \parallel ct_B \parallel \tau_B[0:3]$

$\tau_B \leftarrow \mathsf{CBCMAC}_{K^1_{mac},K^2_{mac}}^{IV_B}(ad_B \parallel ct_B)$

расшифровка ct_B

$IV_A \leftarrow \tau_B$

..... Раунд передачи сообщений завершен .....

Схема модификации защищенного канала

Контроллер $[SCBK]$		**Считыватель** $[SCBK]$
$RND_A \xleftarrow{u} \{0,1\}^{rlen}$	$\xrightarrow{RND_A}$	$RND_B \xleftarrow{u} \{0,1\}^{rlen}$
		$K_{enc} \leftarrow \mathsf{KDF}_{SCBK}(\text{"key iv"}, RND_A \parallel RND_B)$
выработать K_{enc}	$\xleftarrow{RND_B, Crypto_{AB}}$	$Crypto_{AB} \leftarrow \mathsf{E}_{K_{enc}}(RND_A \parallel RND_B)$
проверить корректность		
$Crypto_{BA} \leftarrow \mathsf{E}_{K_{enc}}(RND_B \parallel RND_A)$	$\xrightarrow{Crypto_{BA}}$	проверить корректность
	$\xleftarrow{osdp_{ACK}}$	
..... Процедура установки ключей завершена		
$ct_A \leftarrow \mathsf{MGM}^0_{K_{enc}}(seqnum, ad_A, m_A)$	$\xrightarrow{ad_A \parallel ct_A}$	расшифрование ct_A
расшифрование ct_B	$\xleftarrow{ad_B \parallel ct_B}$	$ct_B \leftarrow \mathsf{MGM}^1_{K_{enc}}(seqnum, ad_B, m_B)$
..... Раунд передачи сообщений завершен		

Сравнение

	OSDP	Количество вызовов	Модификация OSDP	Количество вызовов
Инициализация защищенного канала	AES128-ECB	12	*HMAC*	2
			Kuznechik-*ECB*	4
Шифрование пакетов	AES128-CBC	1	Kuznechik-*MGM*	1
	AES128-CBC_MAC	1		

Заключение

#1

Заменены зарубежные криптоалгоритмы на российские

#2

Сохранена структура передаваемых данных и количество пересылок пакетов в протоколе

Спасибо
за внимание!

Компания Актив

info@rutoken.ru

www.rutoken.ru
www.aktiv-company.ru

+7 495 925-77-90

РусКрипто