**Сервер персонализации**

HS.exe

 *Руководство оператора*

Оглавление

|  |  |
| --- | --- |
| 1. Назначение
 | 3 |
| 1. Описание работы
 | 4 |
| 1. Настройка параметров сервера персонализации
 | 5 |
| 1. Параметры файла скрипта
 | 6 |
|  |  |
|  |  |

1. Назначение.

Программа предназначена для выполнения скриптов персонализации чиповых карт, криптографических операций на HSM типа SafeNet (Eracom), Thales, Racal, а также осуществляет взаимодействие с программами управления смарт-модулями на эмбоссерах и программой подготовки данных.



# Описание работы

Принцип работы основан на обмене сообщениями в специальном протоколе между клиентскими программами и сервером.

Сообщения требующие работы HSM, сервер интерпретирует в команды соответствующего устройства. Сервер персонализации может работать одновременно с несколькими устройствами HSM разного типа. Количество подключаемых клиентов ограниченно только свойствами TCP/IP.

Встроенный в сервер интерпретатор скриптов позволяет одновременно выполнять необходимое количество скриптов персонализации различных чиповых карт с необходимой криптографией на устройствах чтения-записи смарт карт разного типа. Язык написания скриптов специально разработан для работы с чиповыми картами и поддерживает весь необходимый функционал.

# Настройка параметров сервера персонализации

Для инициализации параметров сервера используется файл “HS.INI”. Файл должен находиться в одной директории с “HS.EXE”.

Структура файла следующая:

|  |  |
| --- | --- |
| Секция [OPTIONS] Параметры:  |  |
|  LOG=ON  |  (default = OFF) - ведение лога работы сервера  |
|  FM=2  |  (default = -1) - параметры функционального модуля (далее ФМ) Eracom.  -1 - отсутствие устройства Eracom. Применяется для работы только с HSM Thales, Racal при отсутствие Eracom  1. - отсутствие ФМ модуля Eracom. Работа с HSM Eracom только со стандартной прошивкой, а также с Thales,Racal

 1. - работа только с ФМ Eracom, а также с Thales,

Racal  1. - работа с ФМ и стандартной прошивкой

Eracom, а также с Thales, Racal   |
|  TH\_HEADER=1234  |  (default = 1234) – заголовок сообщений для Thales, Racal Значение любое. Длина определяется настройкой соответствующего HSM  |
|  TOKEN=0  |  (default = 0) - номер рабочего токена Eracom  |
|  ZONE=IVK  |  (default = IVK) - свойство ключей токена Eracom  |
|  LOGIN=ON  |  (default = OFF) - выполнение аутентификации сервера при подключении к Eracom. Используется “user password” рабочего токена Eracom  |

При установке программы на компьютер необходимо скопировать в рабочую директорию файлы: hs.exe, hs.ini, cryptoki.dll, eracom.dll, а также создать в ней директории LOG, SCRIPTS, OUT.

# 4.Параметры файла скрипта

Файл скрипта имеет структуру INI файла.

Состоит из следующих секций:

[OPTIONS] - общие параметры Параметры:

## DATA\_TYPE=AHEX (default = AHEX ) - Формат входных данных

AHEX - текстовый, каждый байт представлен двумя HEX символами

 BIN - бинарный, каждый байт

соответствует одному символу

LOG=1 (default = 1) - запись информации о работе интерпритатора в лог файл.

1. выкл.
2. вкл.

[READER] - параметры для настольных ридеров и устройств чтения-записи чиповых карт настольных эмбосеров и принтеров.

Параметры:

|  |  |
| --- | --- |
| Type=0  | (default = 0) - Тип ридера  1. – PC\SC
2. – RS-232

  |
| Index=0  | (default = 0) - Индекс в списке PC/SC устройств   |
| NCom=1  | (default = 1) - Номер ком порта для RS-232   |
| Protocol=0  | (default = 0) - Протокол для RS-232  1. – GBP
2. – TLP
3. – KDE

  |
| Card=0  | (default = 0) - Тип карты( для PC/SC не надо) 1. - ISO\_368MHZ
2. - ISO\_737MHZ
3. - GPM\_2K
4. - GPM\_8K
5. - OTHER\_SYNCH
 |

 CardBaud=4 (default = 4) - Скорость карты(для GBP)

1. – 76800
2. – 38400
3. – 19200
4. – 9600
5. – 4800
6. – 2400
7. - 1200

 Baud=9600 (default = 9600) - Скорость порта RS-232

 Bits=8 (default = 8) - Кол-во бит данных RS-232

 Parity=0 (default = 0)- Проверка четности RS-232

1. – none
2. – odd
3. – even
4. – bit0
5. – bit1

 StopBit=0 (default = 0) - Стоп бит RS-232

1. - 1
2. - 1,5
3. - 2

[SERVER] - Параметры сервера персонализации Параметры:

 IpPort=1600 (default = 1600) - Номер порта

##  IpAddr=127.0.0.1 (default = 127.0.0.1) - IP адрес

[CONSTANT] - Секция определения констант Параметры:

Имя = значение

[VAR] - Секция определения переменных Параметры:

Имя = индекс

[KEYS] - Секция определения ключей Параметры:

Имя = значение

[IMPLEMENTATION] - Секция кода скрипта Параметры:

Строка скрипта 1=

## ……………………

 Строка скрипта N=