Сервер сетевых лицензий

Guardant Net – это технология защиты и лицензирования сетевых приложений с использованием электронных ключей Guardant. Основными компонентами Guardant Net являются:

Сетевой ключ	Ключ для защиты и лицензирования сетевого приложения
Сервер Guardant Net	Утилита, обрабатывающая и передающая запросы от клиента к ключу и обратно
Клиент	Защищенное приложение, которое обращается к серверу ключа с удаленного компьютера
Сетевой протокол	Протокол, по которому происходит обмен между сервером и клиентом

К важным понятиям Guardant Net также следует добавить **сетевой ресурс ключей** и его **распределение** (в том числе, при работе с многомодульными программными комплексами).

1. Сетевые ключи

Сетевые ключи Guardant предназначены для защиты и лицензирования сетевых приложений. Под лицензированием подразумевается ограничение количества одновременно работающих в ЛВС клиентских приложений. Цель лицензирования – запретить запуск клиентов сверх разрешенного разработчиком количества. Ресурс лицензий записывается разработчиком в память сетевого ключа. Для защиты и лицензирования сетевого продукта достаточно использовать один сетевой ключ Guardant на всю локальную сеть. Он может быть установлен на любую рабочую станцию или сервер. К сетевым ключам относятся следующие модели:

Модель ключа	**Основные характеристики**				
	Объем памяти	**Платформа**	**Аппаратные алгоритмы**	**HID**	**RTC**
Sign Net / Time Net	4096 Б	Windows, Linux (Wine)	AES, GSII64, ECC160, SHA256, HASH64	+	-/+
Net III (устаревшая)	2048 Б	Windows	GSII64; HASH64, RND64	-	-
Net II (устаревшая)	256 Б	Windows	GSII64; Stealth I	-	-

1.1. Сетевой ресурс ключей и его распределение

Каждый сетевой ключ обладает определенным сетевым ресурсом, который позволяет ограничивать число одновременно запущенных клиентов. Сетевой ресурс ключа может распределяться по рабочим станциям, процессам или хэндлам Guardant API, в зависимости от решаемой задачи. Для многомодульных приложений используется система управления лицензиями, когда каждому модулю приложения дополнительно присваивается отдельный сетевой ресурс лицензий.

1.2. Сетевой протокол

Сетевые ключи Guardant могут работать в любых локальных сетях с интерфейсом TCP/IP. Однако ключи устаревших моделей (см. таблицу выше) не поддерживают работу в ОС Linux и для них сервер ключа должен быть установлен на компьютере под управлением ОС семейства Windows (либо в среде wine@etersoft под Linux).

2. Сервер Guardant Net

Защищенные сетевые приложения не могут обращаться непосредственно к сетевому ключу. Связующим звеном между защищенным приложением (клиентом) и сетевым ключом выступает специальная утилита – программный сервер Guardant Net (файл **glds.exe**). Сервер обеспечивает прохождение запросов от клиента непосредственно к ключу и обратно по правилам сетевого протокола TCP/IP.

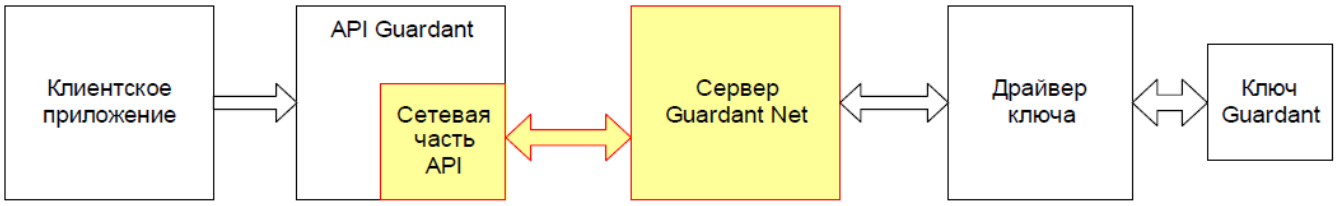
> Сервер Guardant Net должен быть загружен на том же компьютере, к которому подсоединен сетевой электронный ключ.
> В одной директории с **glds.exe** должен находиться конфигурационный файл **grdsrv.ini**, в котором хранятся текущие настройки сервера ключа.

3. Клиент Guardant Net

Защищенное приложение (клиент) при запуске должно найти сервер ключа и зарегистрироваться на нем, чтобы продолжить работу. В зависимости от схемы распределения лицензий в качестве клиента может выступать процесс (копия) приложения, рабочая станция или хэндл (копия экземпляра GrdAPI, использующаяся при защите). Каждому клиенту после регистрации на сервере ключа выделяется единица сетевого ресурса.
Для работы клиенту Guardant Net не требуется установка драйвера Guardant, т. к. он не обращается непосредственно к ключу. В одной директории с клиентским приложением должен находиться конфигурационный файл **gnclient.ini**, в котором хранятся настройки клиента.

4. Принцип работы сетевой защиты

Для работы защищенного приложения в локальной сети необходимо и достаточно установить один сетевой электронный ключ на любую рабочую станцию или сервер.
Работу с электронным ключом по сети обеспечивает клиентская (Guardant Net API и/или «вакцина» автоматической защиты) и серверная (сервер Guardant Net) части ПО Guardant. Для связи клиентской и серверной частей ПО Guardant Net необходимо настроить конфигурационные файлы клиента (gnclient.ini) и сервера ключа (grdsrv.ini).



При запуске сервер Guardant Net считывает и запоминает сетевые ресурсы и другие параметры ключей, подсоединенных к данному компьютеру. Защищенный клиент, чтобы начать работу с ключом, должен зарегистрироваться на сервере (выполнить функцию GrdLogin). В процессе регистрации клиента сервер проверяет, подсоединен ли к компьютеру ключ с запрашиваемыми параметрами, и уменьшает на 1 значение его сетевого ресурса. В противном случае он возвращает клиенту ошибку «Электронный ключ не найден». После успешной регистрации приложение может выполнять с ключом все доступные операции. При завершении своей работы приложение снимает свою регистрацию с сервера (выполняет функцию GrdLogout). В процессе снятия регистрации производится возврат (увеличение на 1) сетевого ресурса соответствующего ключа. Если клиент запрашивает регистрацию на сервере Guardant Net в тот момент, когда сетевой ресурс ключа уже исчерпан (равен 0), сервер вернет соответствующую ошибку, и данная копия приложения не будет запущена.

Сетевые ресурсы корректируются не в памяти ключей, а в памяти сервера. Это дает гарантию сохранности сетевого ресурса ключа при аппаратных сбоях в сети, «подвисании» рабочих станций и т.п.

5. Содержание раздела

- Ресурс лицензий ключа
- Таблица лицензий
- Управление лицензиями
- Сервер Guardant Net Windows
- Сервер Guardant Net Linux
- Клиент Guardant Net
- Повышение надежности сетевого обмена