



# iPhone и виртуальные частные сети (VPN)



## Протоколы VPN

- Cisco IPSec
- L2TP/IPSec
- PPTP

## Методы аутентификации

- Пароль (MS-CHAPv2)
- RSA SecurID
- CRYPTOCard
- Сертификаты (PKCS1, PKCS12)
- Общий секрет

Для безопасного доступа к корпоративным сетям в iPhone используются самые популярные стандартные протоколы VPN. ПО iPhone 2.0 поддерживает Cisco IPSec, L2TP через IPSec, а также PPTP. Если в организации поддерживается один из этих протоколов, для подключения iPhone к VPN не требуется никакой дополнительной настройки сети или приложений сторонних разработчиков.

В развёртывании Cisco IPSec можно использовать аутентификацию на основе стандартных цифровых сертификатов x.509 (PKCS1, PKCS12). Для реализации двухфакторного механизма аутентификации iPhone поддерживает RSA SecurID, а также CRYPTOCard. Пользователи вводят PIN-код и сгенерированный одноразовый пароль непосредственно на iPhone во время установки подключения VPN.

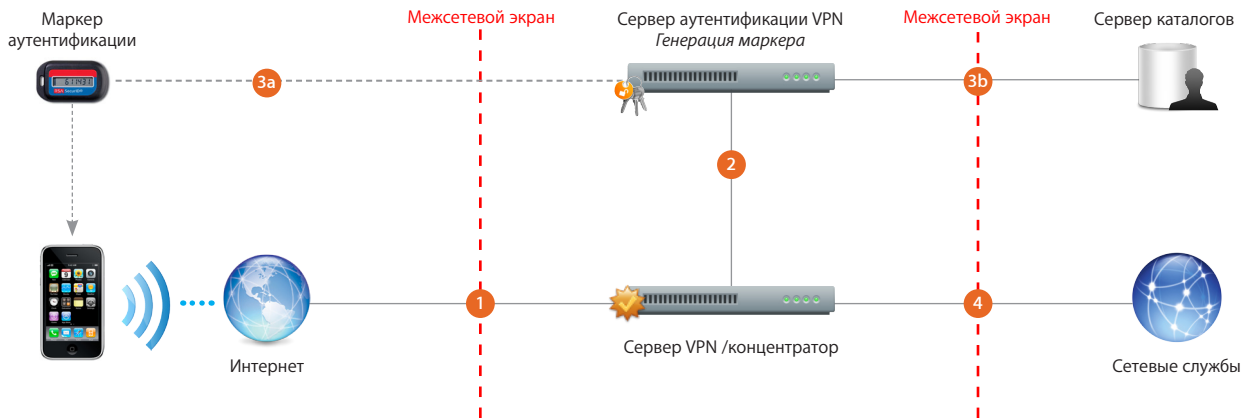
iPhone поддерживает аутентификацию по секретному коду для развёртываний Cisco IPSec и L2TP/IPSec. А для обычной аутентификации по имени пользователя и паролю iPhone поддерживает MS-CHAPv2. Независимо от метода аутентификации предварительно заданные настройки VPN можно передать пользователям через профиль конфигурации или ввести непосредственно на iPhone.

## Настройка VPN

- Поскольку iPhone интегрируется с большинством существующих сетей VPN, чтобы разрешить ему доступ к сети, потребуется минимальная настройка. В рамках подготовки к развёртыванию рекомендуется убедиться, что iPhone совместим с существующими протоколами VPN и методами аутентификации вашей компании.
- Проверьте совместимость существующих стандартов с концентраторами VPN. Также рекомендуется проверить путь к серверу аутентификации RADIUS или VPN и убедиться, что поддерживаемые на iPhone стандарты включены в существующей реализации.
- Если вы планируете использовать аутентификацию на основе сертификатов, убедитесь, что инфраструктура открытых ключей настроена на поддержку сертификатов устройства и пользователя с помощью соответствующего процесса распространения ключей.
- Проверьте формат сертификата и совместимость сервера аутентификации. iPhone поддерживает PKCS1 (.cer, .crt, .der) и PKCS12 (.p12, .pfx).
- Подтвердите у поставщика решения, что программное обеспечение и оборудование соответствуют новейшим обновлениям для системы безопасности и прошивки.
- Дополнительную документацию относительно протокола Cisco IPSec и спецификации можно найти по адресу [www.cisco.com/ru](http://www.cisco.com/ru).

## Сценарий развёртывания VPN

На этом рисунке изображено типичное развёртывание с помощью сервера/концентратора VPN, а также сервера аутентификации VPN, который контролирует доступ к корпоративным сетевым службам.



- 1 iPhone запрашивает доступ к сетевым службам (обычно через подключение PPP).
- 2 Сервер/концентратор VPN получает запрос и передаёт его серверу аутентификации.
- 3a В среде двухфакторной аутентификации сервер аутентификации затем производит синхронизированную во времени генерацию ключа маркера при помощи сервера ключей. Если применяется метод сертификата или пароля, то для аутентификации необходимо подтверждение пользователя.
- 3b После аутентификации пользователя сервер аутентификации подтверждает политики сетевого доступа пользователя и группы.
- 4 После подтверждения политик пользователя и группы сервер VPN обеспечивает туннельный зашифрованный доступ к сетевым службам (обычно через IPSec).