Лучшие практики:

1. Защита соединения SSL сертификатом. SSL (англ. Secure Sockets Layer — уровень защищённых сокетов) — криптографический протокол, который подразумевает более безопасную связь. Он использует асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений.
2. Использование ключа доступа вместо пары логин/пароль. Считается стандартом сетевой безопасности:
    - Ключ доступа генерируется автоматически, имеет достаточно крипто устойчивую длину и набор символов (пароль пользователя может быть очень простым)
    - Ключ доступа привязан к конкретному устройству, т.е. компрометация ключа не даст злоумышленнику доступ ко всему аккаунту
    - Ключ доступа может быть сброшен не требуя смены пароля, потребуется лишь заново авторизоваться
3. Advanced Encryption Standard (AES-256), симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 256 бит). В июне 2003 года Агентство национальной безопасности США постановило, что шифр AES является достаточно надёжным, чтобы использовать его для защиты сведений, составляющих государственную тайну (англ. classified information). Вплоть до уровня SECRET было разрешено использовать ключи длиной 128 бит, для уровня TOP SECRET требовались ключи длиной 192 и 256 бит. По сегодняшний день AES является одним из самых распространённых алгоритмов симметричного шифрования.