Краткая история

Пароли, логины и хеши паролей не передаются по сети.

KDC сохраняет криптоключи всех пользователей

Синхронизировано время на всех устройствах

Два домена могут быть подключены, для этого KDC регистрируются друг в друге, как пользователи (TGT-шками)

Используется в Windows Active Directory, МинОбороны США, университеты и т.д.

**Плюсы и минусы:**

* TGT живет 8-10 часов —> небольная нагрузка на сеть
* Взаимная аутентификация
* Отсутствие пересылки важных данных по сети
* Каждый пользователь может просматривать только предназначающиеся ему сообщения

**Минусы:**

* Централизованное хранение всех ключей
* «Керберизация» приложений
* Строгие требования к синхронизации времени

**Виды атак:**

* Pass-the-ticket – подделка TGT
* Золотой билет – подделка TGT администратора
* Серебряный билет – подделка TGS
* Brute Force
* Бэкдор во вредоносном ПО