FreeIPA
LDAP+Kerberos

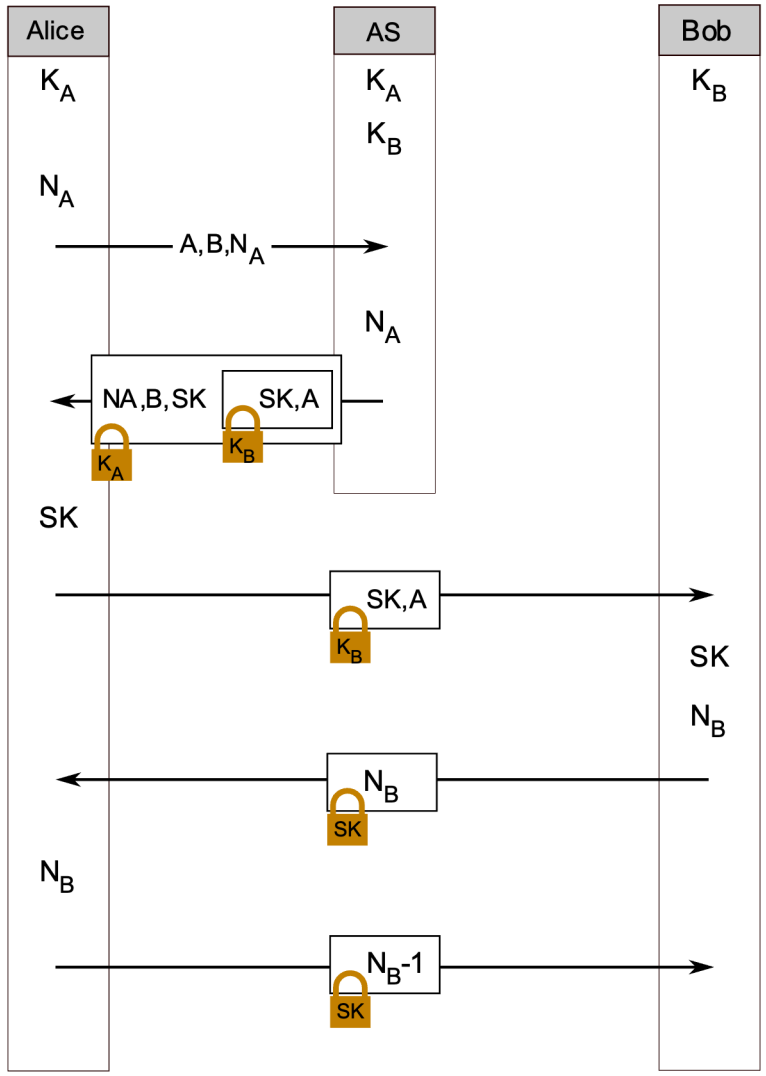
Single sign-on

- Очень много пользователей
- Много серверов
- Если все будут аутентифицироваться через центральный сервер (например, LDAP), этому серверу хорошо не будет
  - Реплики центральных серверов (LM/NT4 BDC, openldap syncrepl)
  - Кэширование креденшиалов на серверах (NT4) - небезопасно
  - Схема (алгоритм) Нидхама-Шредера

Схема Нидхама-Шредера

- K_A и K_B – разделяемые секреты (обычно просто хэш пароля)
- N_X – nonce (number used once), некая уникальная битовая строка
- SK – Session Key, разделяемый между Алисой и Бобом секрет
- SK,A – тикет (зашифрованный K_B)

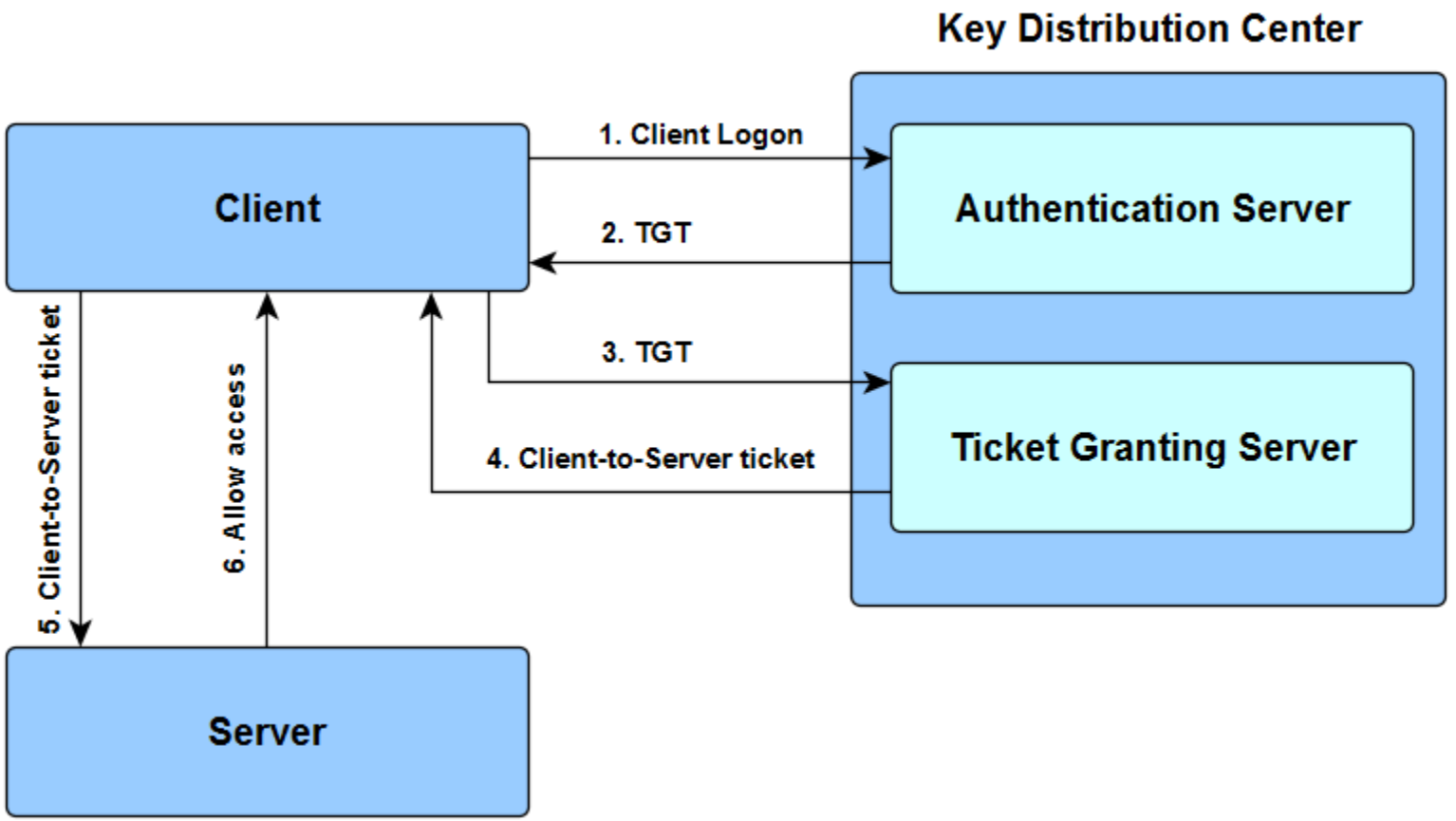
Схема (в т.ч. в виде варианта на публичных ключах) лежит в основе современных протоколов SSO



Kerberos

- Такая собачка из греческой мифологии
  (в русских переводах известна как Цербер)
- Разработан в конце 80х в MIT в рамках проекта Athena
- RFC 1510/4120
- Open source
- Основан на схеме Нидхама-Шредера
- Лежит в основе MS Active Directory

Kerberos под капотом



Зачем нужен отдельный AS?

- Регистрация учетных записей (в том числе machine account)
- Смена пароля
- Преаутентификация (ticket granting ticket)
- Схема Нидхама-Шредера в чистом виде этого не содержит

Kerberos в Linux

- Наиболее известное применение – аутентифицированная NFS
- Также аутентификация SMB, HTTP, ssh и др.
- Обычно используется совместно с LDAP сервером
- Можно развернуть самостоятельно
  (есть все нужные пакеты в большинстве дистрибутивов)
- Сложно настроить самостоятельно
  - Нужна интеграция с DNS (как в Active Directory)
- FreeIPA: интегрированный сервис, включающий
  - LDAP
  - DNS
  - Kerberos
  - веб интерфейс для управления всем этим

Для установки Linux в домен FreeIPA

- Должна быть делегационная запись на домен в DNS
- Для демонстрации проще,
  чтобы линукс использовал DNS FreeIPA
- В пакет клиента IPA входит утилита, которая настраивает LDAP и Kerberos клиенты и создает учетную запись компьютера в домене

Что после установки

- Получение TGT осуществляется утилитой kinit.
- Чтобы получить тикет, не обязательно, чтобы учетная запись Linux была зарегистрирована в домене Kerberos
- Но для учетных записей из домена kinit обычно происходит автоматически при входе
- Тикеты сохраняются в /tmp в каталоге с правами только для этого пользователя Linux
- Если /tmp на tmpfs, они потеряются при выключении/перезагрузке (вообще-то это хорошо)

Демонстрация/упражнение

- Установка компьютера Astra Linux в домен IPA
- Аутентификация на контроллере домена IPA по ssh

Какое все это имеет отношение к интеграции с AD?

- Active Directory, в конечном итоге, тоже LDAP+Kerberos
- Все схемы интеграции под капотом используют те же или перекрывающиеся наборы средств
- Еще используется winbind для генерации атрибутов учетных записей Unix (uid, gid, home directory, shell)

Дополнительно: интеграция FreeIPA с AD

- Интеграция подразумевает создание доменного траста между AD и FreeIPA
- Пользователи AD смогут заходить на компьютеры домена IPA по ssh
- С компьютеров домена IPA можно будет монтировать шары SMB из домена AD