??? ???????? Kerberos — ?????? ??? ???????? ???????

??????????

Kerberos — сетевой протокол аутентификации на основе тикетов (RFC 4120). Позволяет пользователям доказывать свою идентичность сервисам без передачи пароля по сети.

???????? ??????????

Компонент	Описание
KDC (Key Distribution Center)	Центр выдачи тикетов, обычно совмещён с AD
AS (Authentication Service)	Выдаёт TGT после проверки пароля
TGS (Ticket Granting Service)	Выдаёт тикеты сервисов на основе TGT
TGT (Ticket Granting Ticket)	Первичный тикет, подтверждает личность пользователя
ST (Service Ticket)	Тикет для доступа к конкретному сервису
Realm	Административный домен Kerberos (обычно = DNS-домен, UPPER CASE)

??????? ????????????

```
1. Клиент  →  AS:   AS-REQ (имя пользователя)
2. AS      →  Клиент: AS-REP (TGT, зашифрован ключом KDC)
3. Клиент  →  TGS:  TGS-REQ (TGT + имя сервиса)
4. TGS     →  Клиент: TGS-REP (Service Ticket)
5. Клиент  →  Сервис: AP-REQ (Service Ticket)
6. Сервис  →  Клиент: AP-REP (подтверждение)
```

?????? ???? ?????????? (SSO)

После получения TGT (шаги 1–2, выполняются при входе в Windows/Linux) все последующие обращения к сервисам (шаги 3–6) происходят автоматически — пользователь не вводит пароль повторно.

TGT имеет срок жизни — как правило, 8–10 часов (настраивается в политиках домена). По истечении требуется повторная аутентификация или продление (renewal).

???????? ????????

- Пароль пользователя **никогда** не передаётся по сети.
- Используется симметричное шифрование (AES-256 в современных реализациях).
- Все тикеты ограничены по времени (timestamp + skew до 5 минут).
- Расхождение системных часов более 5 минут приводит к ошибке `KRB_AP_ERR_SKEW`.

????? ? SSO ? ???????

Принтум может использовать Kerberos/GSSAPI для прозрачной аутентификации пользователей в среде Active Directory — пользователь, вошедший в домен, получает доступ к сервисам Принтум без повторного ввода пароля.

TODO: уточнить — поддерживается ли Kerberos SSO напрямую или только через промежуточный IdP (например, ADFS/Keycloak).

Revision #5
Created 2026-05-10 11:16:04 UTC by DD
Updated 2026-06-01 13:20:07 UTC by Андрей Толкачев