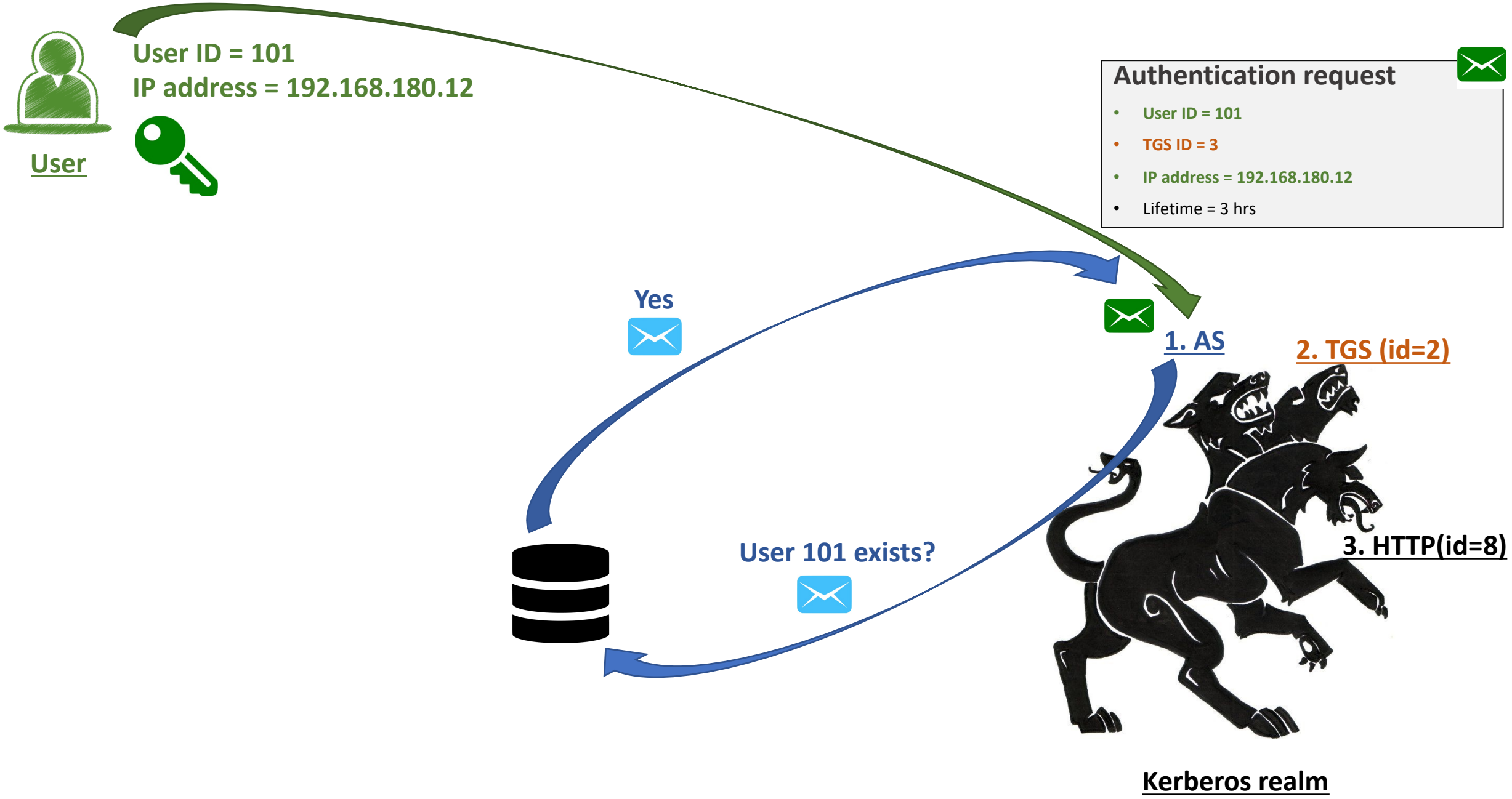
Kerberos


User ID = 101
IP address = 192.168.180.12
User
Authentication request
User ID = 101
TGS ID = 3
IP address = 192.168.180.12
Lifetime = 3 hrs
1. AS
2. TGS (id=2)
3. HTTP(id=8)
Yes
User 101 exists?
Kerberos realm

User ID = 101
IP address = 192.168.180.12

User

AS generates a random session key for TGS

1. AS

2. TGS (id=2)

3. HTTP(id=8)

Kerberos realm

User ID = 101
IP address = 192.168.180.12

User

hash(Password + salt)

Ticket granting ticket

- User ID = 101
- TGS ID = 3
- Timestamp
- Network address
- Lifetime = 3 hrs
- TGS session key

Response

- TGS ID = 3
- Timestamp
- Lifetime = 3 hrs
- TGS session key

1. AS

2. TGS (id=2)

3. HTTP(id=8)

Kerberos realm

Ticket granting ticket

User ID = 101
IP address = 192.168.180.12

User

Response

- TGS ID = 3
- Timestamp
- Lifetime = 3 hrs
- TGS session key

1. AS

2. TGS (id=2)

3. HTTP(id=8)

Kerberos realm

User ID = 101
IP address = 192.168.180.12

User

1. AS

2. TGS (id=2)

3. HTTP(id=8)

Kerberos realm

Request

- Service ID = 8
- Lifetime = 1hr

Authenticator

- User ID = 101
- timestamp

Ticket granting ticket

User ID = 101
IP address = 192.168.180.12

User

Ticket granting ticket

- User ID = 101
- TGS ID = 3
- Timestamp
- Network address
- Lifetime = 3 hrs
- TGS session key

Authenticator

- User ID = 101
- timestamp

1. AS

2. TGS (id=2)

3. HTTP(id=8)

Kerberos realm

User ID = 101
IP address = 192.168.180.12

User

In range?

1. Сравнить **User ID**
2. Сравнить timestamp
3. Проверить, не истекло ли время действия тикета
4. Проверить свой кэш
5. Проверить, что **user IP** в пределах сети

Ticket granting ticket

- User ID = 101
- TGS ID = 3
- Timestamp
- Network address
- Lifetime = 3 hrs
- TGS session key

Cmp()

Cmp()

Expired?

Authenticator

- User ID = 101
- timestamp

1. AS

2. TGS (id=2)

3. HTTP(id=8)

TGS cache

Auth in cache?

Kerberos realm

User ID = 101
IP address = 192.168.180.12

User

TGS generates a random session key for HTTP service

Client ID + timestamp

1. AS

2. TGS (id=2)

3. HTTP(id=8)

Kerberos realm

User ID = 101
IP address = 192.168.180.12

User

1. AS

2. TGS (id=2)

HTTP Service ticket

- User ID = 101
- HTTP service ID = 8
- Timestamp
- Network address
- Lifetime = 3 hrs
- HTTP service session key

Response

- HTTP service ID = 8
- Timestamp
- Lifetime = 3 hrs
- HTTP service session key

3. HTTP(id=8)

Kerberos realm

User ID = 101
IP address = 192.168.180.12

User

HTTP Service ticket

Response

- HTTP service ID = 8
- Timestamp
- Lifetime = 3 hrs
- HTTP service session key

1. AS

2. TGS (id=2)

3. HTTP(id=8)

Kerberos realm

User ID = 101
IP address = 192.168.180.12

User

HTTP Service ticket

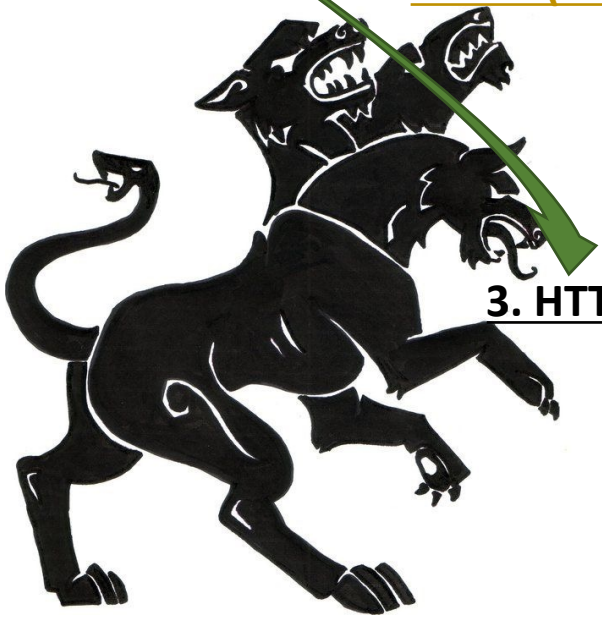
Authenticator

- User ID = 101
- timestamp

1. AS

2. TGS (id=2)

3. HTTP(id=8)



Kerberos realm

User ID = 101
IP address = 192.168.180.12

User

1. Сравнить **User ID**
2. Сравнить timestamp
3. Проверить, не истекло ли время действия тикета
4. Проверить свой кэш
5. Проверить, что **user IP** в пределах сети

In range?

HTTP Service ticket

- User ID = 101
- HTTP service ID = 8
- Timestamp
- Network address
- Lifetime = 3 hrs
- HTTP service session key

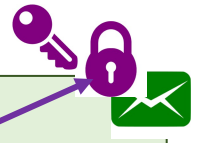
Cmp()

Cmp()

Expired?

Authenticator

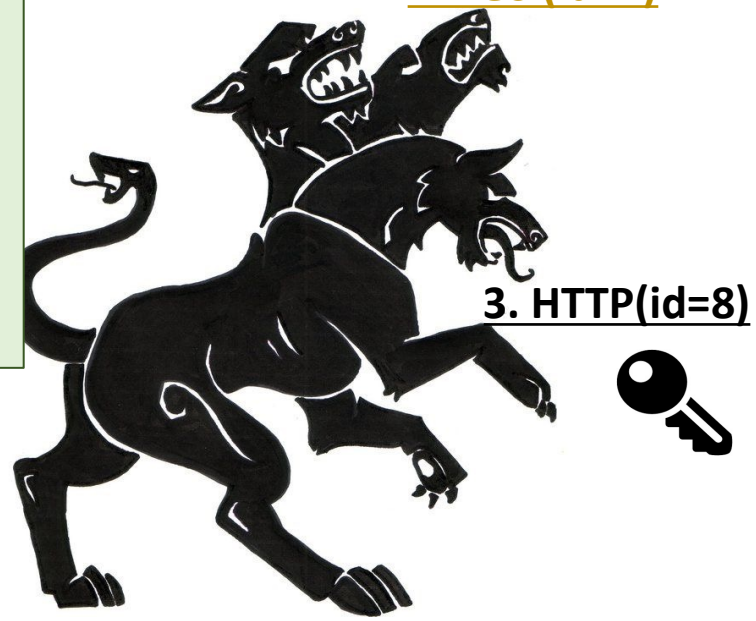
- User ID = 101
- timestamp



1. AS

2. TGS (id=2)

3. HTTP(id=8)



HTTP cache

Auth in cache?

Kerberos realm

User ID = 101
IP address = 192.168.180.12

User

Authenticator

- Server ID = 8
- timestamp

1. AS

2. TGS (id=2)

3. HTTP(id=8)

Kerberos realm

Golden ticket vs Silver ticket