Grupo 8

TÉCNICO LISBOA

3ª Entrega: Sistema Binas

SISTEMAS DISTRIBUÍDOS

2º SEMESTRE – 2017/2018

Grupo 8

https://github.com/tecnico-distsys/T08-SD18Proj.git

André Fonseca
84698

Diogo D'Andrade
84709

Leonor Loureiro
84736

PROTOCOLO KERBEROS (VERSÃO V5) – VERSÃO SIMPLIFICADA

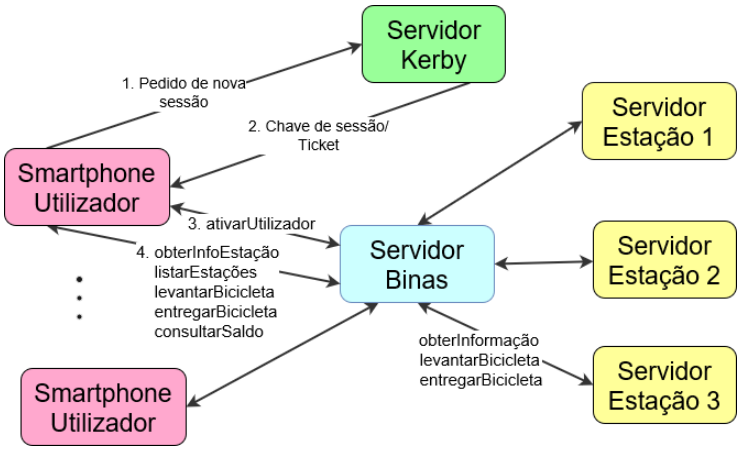

Figura 1 Diagrama da Solução

Login

1. Cliente envia pedido de nova sessão ao servidor Kerby, incluindo no pedido um nonce, n
2. O Kerby retorna
   - a chave de sessão, $\{K_{C,B}, n\}_{Kc}$, e
   - o ticket respetivo, $T = \{C, B, T1, T2, K_{C,B}\}_{KB}$

Acesso ao Binas

3. Cliente decifra a chave de sessão, obtendo $K_{C,B}$
4. Cliente gera um novo autentificador, $A = \{T_{req}\}_{Kc,B}$
5. Cliente gera o resumo do pedido, $S_1 = H(M+K_{C,B})$
6. Cliente invoca a operação ativarUtilizador do servidor Binas, incluindo no pedido:
   - o ticket T,
   - o autentificador A, e
   - o resumo S_1
7. Binas decifra o ticket e verifica a sua frescura.
8. Se o ticket ainda estiver no período de validade,
   i. decifra o resumo S_1,
   ii. computa o resumo S_1', e
   iii. verifica se $S_1=S_1'$
9. Binas executa o pedido
10. Binas decifra o autenticador A, obtendo o request time, T_{req}

Autenticação do Binas

11. Binas gera o resumo da mensagem de resposta, $S_2 = H(M'+K_{C,B})$
12. Binas retorna, incluindo na resposta:
    - o request time, T_{req}, encriptado com a chave de sessão $K_{C,B}$, e
    - o resumo S_2
13. Cliente
    i. decifra o resumo S_2
    ii. computa o resumo $S_2'=H(M'+K_{C,B})$
    iii. verifica se $S_2=S_2'$

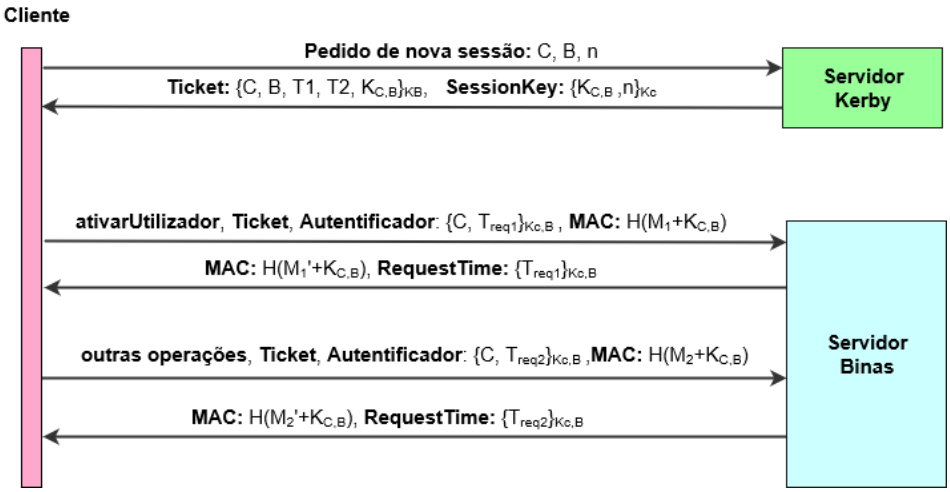

Figura 2: Trocas de Mensagens

SOAP HANDLERS

Cliente:

- Adicionar ao header das mensagens OUTBOUND:
  - **To: Servidor Kerby** (pedido de nova sessão ao Servidor Kerby)
    - *Username* do utilizador
    - *Username* do servidor Binas
    - Nonce
  - **To: Servidor Binas** (invocação de uma operação do Binas)
    - Ticket
    - Autentificador
    - MAC
- Extrair do header das mensagens INBOUND:
  - **From: Servidor Kerby**
    - Ticket
    - SessionKey
  - **From: Servidor Binas**
    - MAC
    - RequestTime

Binas:

- Incluir no header das mensagens OUTBOUND:
  - **To: Cliente**
    - MAC
    - RequestTime
- Extrair do header das mensagens INBOUND:
  - **From: Cliente**
    - Ticket
    - Autenticador
    - MAC