



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 |

Grupo 8

Protocolo Kerberos (versão V5) – Versão Simplificada

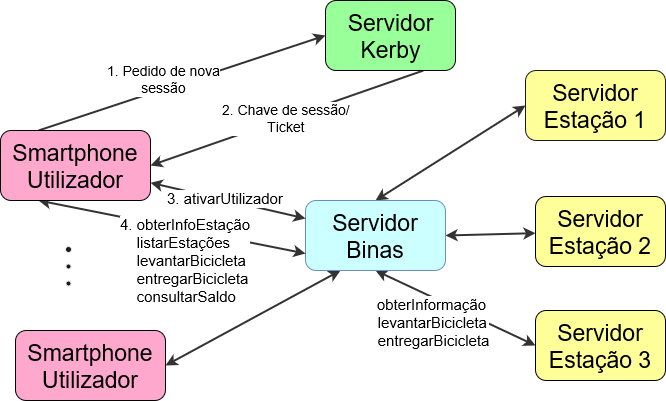


Figura 1 Diagrama da Solução

|  |  |
| --- | --- |
| 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, {KC,B, n}Kc, e * o ticket respetivo, T |
| Acesso ao Binas | 1. Cliente decifra a chave de sessão, obtendo KC,B 2. Cliente gera um novo autentificador, A = {Treq}Kc,B 3. Cliente gera o resumo do pedido, S1 = H(M+KC,B) 4. Cliente invoca a operação ativarUtilizador do servidor Binas, incluindo no pedido:  * o ticket T, * o autentificador A, e * o resumo S1  1. Binas decifra o ticket e verifica a sua frescura. 2. Se o ticket ainda estiver no período de validade, 3. decifra o resumo S1, 4. computa o resumo S1’, e 5. verifica se S1=S1’ 6. Binas executa o pedido 7. Binas decifra o autenticador A, obtendo o request time, Treq |
| Autenticação do Binas | 1. Binas gera o resumo da mensagem de resposta, S2 = H(M’+KC,B) 2. Binas retorna, incluindo na resposta:  * o request time, Treq, encriptado com a chave de sessão KC,B, e * o resumo S2  1. Cliente 2. decifra o resumo S2 3. computa o resumo S2’=H(M’+KC,B) 4. verifica se S2=S2’ |

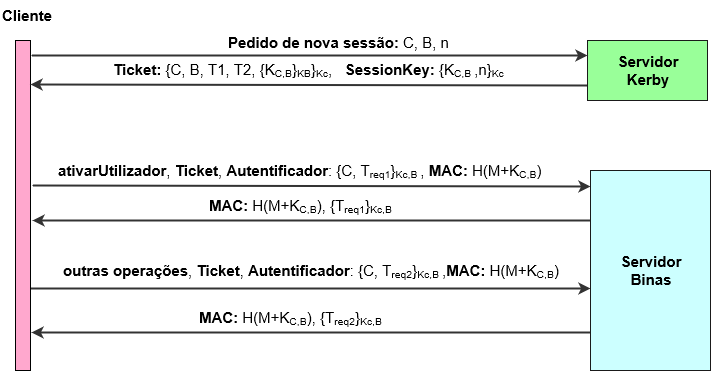


Figura 2: Trocas de Mensagens