Universidade Estadual do Oeste do Paraná - Foz do Iguaçu
Ciência da Computação – Sistemas Operacionais
Professor Shiro

Kerberos

Andre da Silva

Eder Ruiz Maria

Rodrigo Renie Braga

Sumário

- Justificativa
- Segurança
- Kerberos
- Conceitos
- Funcionamento
- Autenticação
- Considerações

Justificativa

- Porque faz-se necessário segurança?
  - Informações sigilosas
    - Interceptação
    - Modificação
    - Interrupção
    - Usurpação
  - Contexto histórico
    - downsize
  - Características do protocolo TCP/IP

Segurança

- Autenticação
- Autorização
- Integridade
- Privacidade

Kerberos

- Cerberos
  - Guardião do portão do inferno
- Protocolo de Comunicação
  - Criado no MIT na década de 80
  - Atua como uma terceira parte

Conceitos

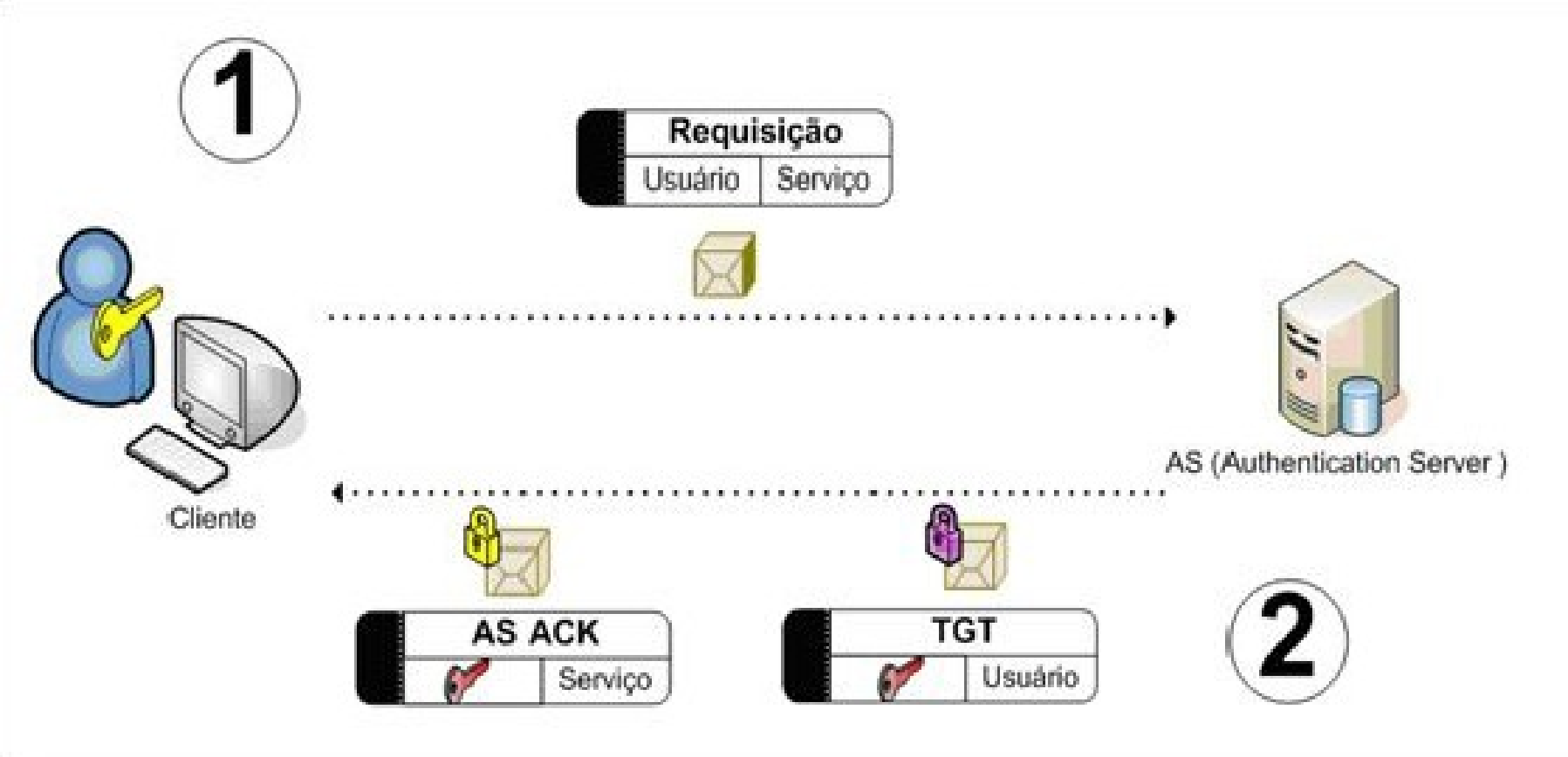
- Criptografia (Simétrica e Assimétrica)
- Principais, realms e tickets
- Key Distribution Center (KDC)
- Authentication Server (AS)
- Tickets Granting Server (TGS)

Funcionamento

- Analogo ao RG
  - Obtenção do RG (cadastramento)
  - Compra de um ingresso para um evento

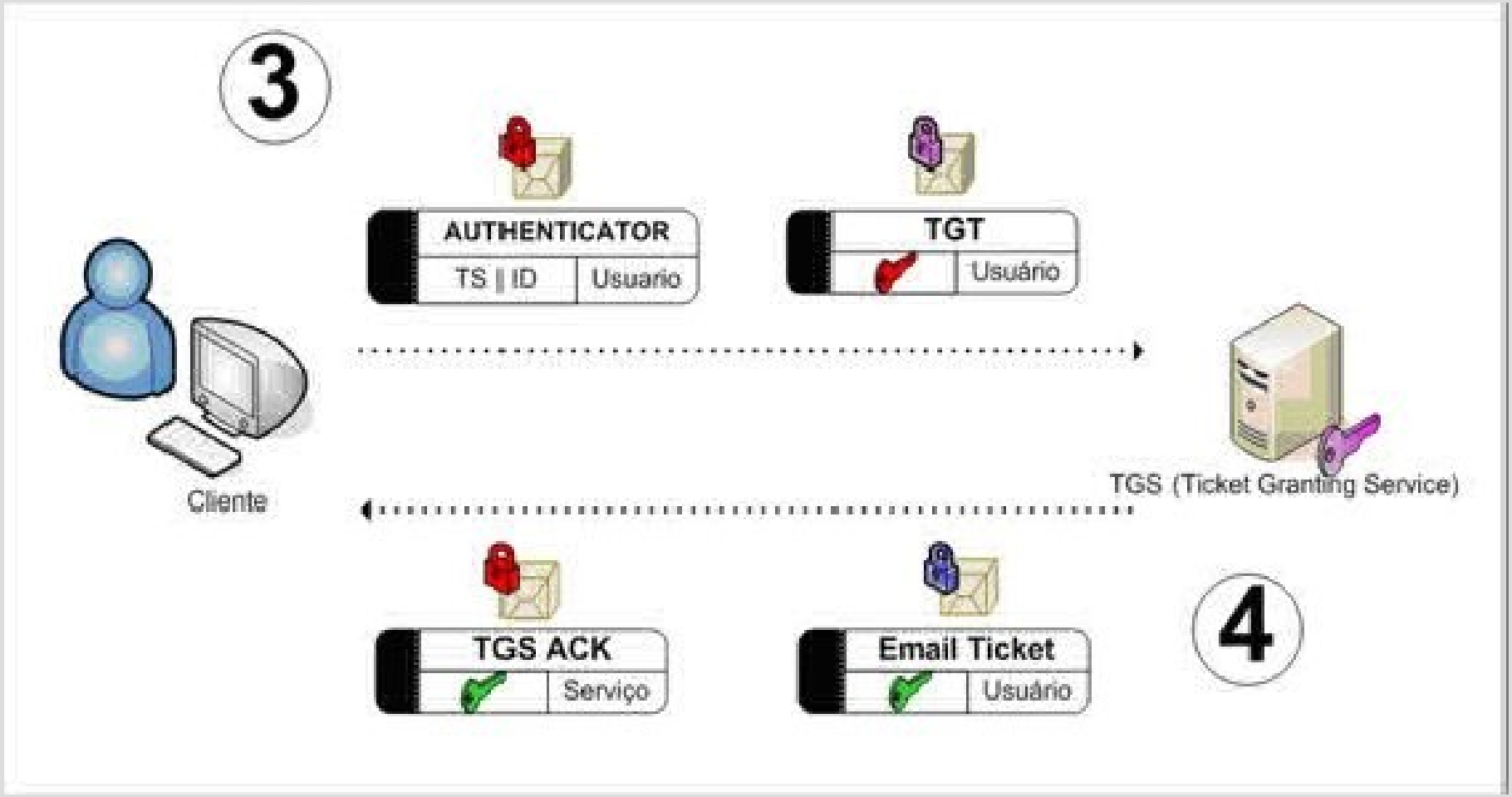
Autenticação

Comunicando-se com o Authentication Server



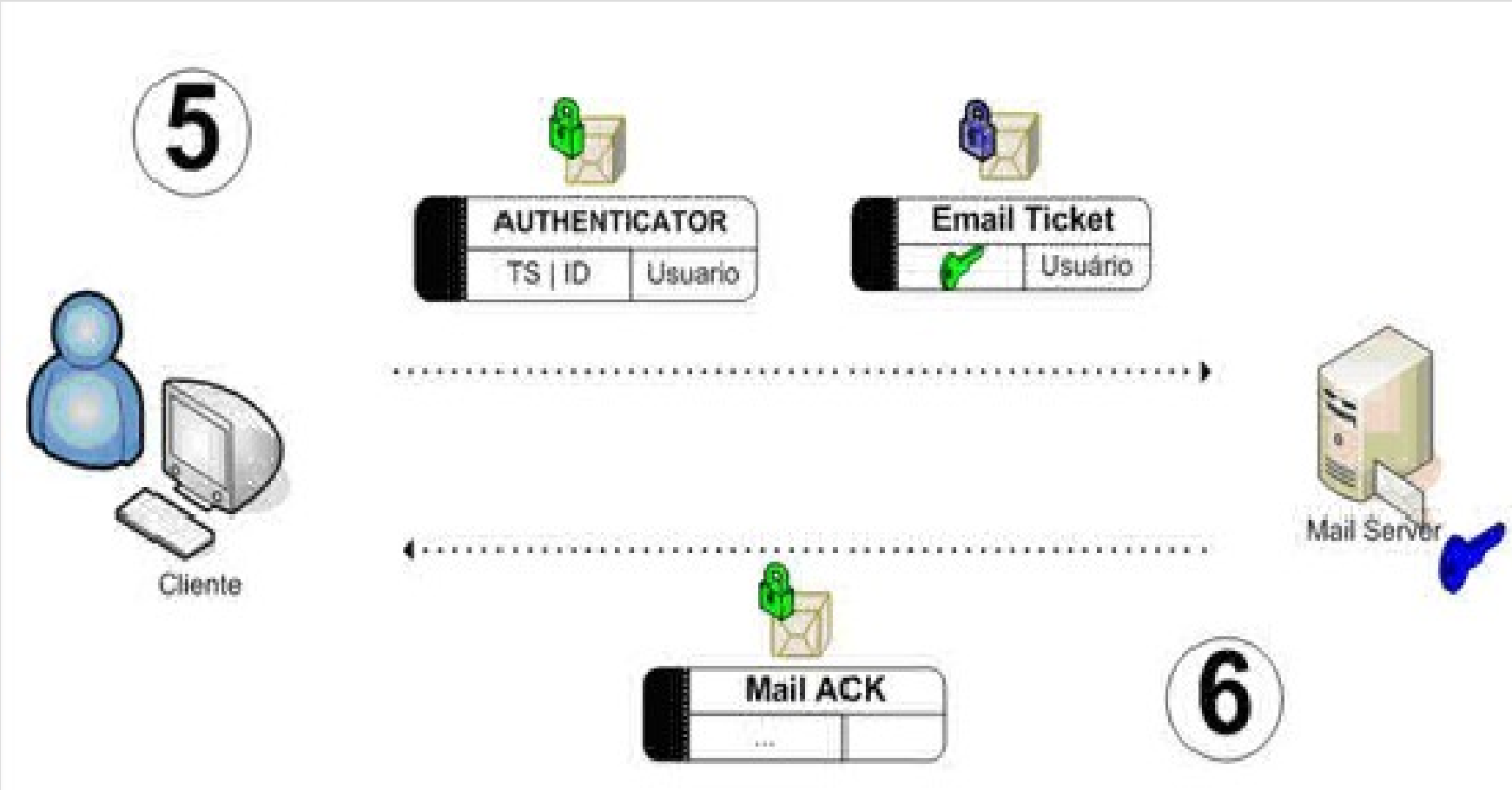
Autenticação (cont.)

Comunicando-se com o Ticket Granting Server



Autenticação (cont.)

Comunicando-se com o Mail Server



Considerações

- O Kerberos garante:
  - Segurança na rede
  - Autenticação Mutua
  - Centralização de Serviços
  - Administração Simples

Considerações (cont.)

- Problemas do Kerberos:
  - Base de dados das chaves
  - Senhas Fracas (amor, sexo, deus, uhet)
  - Sincronização do Relógio (timestamp)

Obrigado!

- Agradecimento ao GNOIA (www.gnoia.org)
- William Merlotto (Jedi)

- Perguntas?