



Desafio 1 e Desafio 2



SEM 1-2019

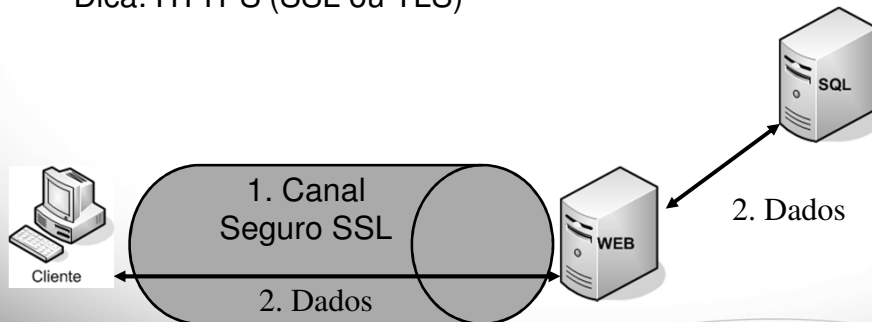
UNIVERSIDADE DO OESTE PAULISTA
UNOESTE
PRESIDENTE PRUDENTE - SP

Contexto

- Considerando que:
 - Sigilo: ambos os esquemas de criptografia conhecidos (simétrico e assimétrico) são adequados baseando-se em algoritmo e tamanho de chave considerados seguros
 - Autenticação: o esquema assimétrico é mais adequado
 - Desempenho computacional (processamento e memória): o esquema simétrico é mais adequado
- Admitindo como premissa
 - Atualmente ambos os esquemas de criptografia simétrico e assimétrico são utilizados na prática para soluções seguras em transações eletrônicas

Desafio 1

- Esquematizar o funcionamento de uma solução segura para transações eletrônicas que ocorrem num serviço baseado em sessão de comunicação on-line
 - Por exemplo, serviço WEB
 - Dica: HTTPS (SSL ou TLS)

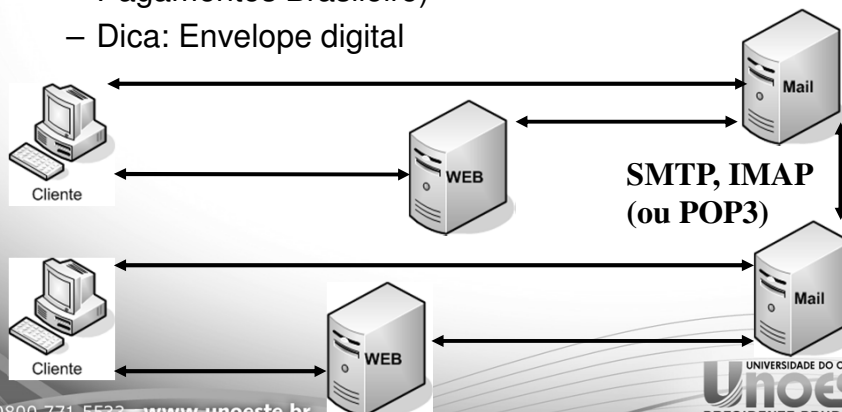


0800-771 5533 — www.unoeste.br

UNIVERSIDADE DO OESTE PAULISTA
UNOESTE
PRESIDENTE PRUDENTE - SP

Desafio 2

- Esquematizar o funcionamento de uma solução segura fim a fim para transações eletrônicas que ocorrem num serviço orientado a troca de mensagens
 - Exemplos, serviço EMAIL e SPB (Sistema de Pagamentos Brasileiro)
 - Dica: Envelope digital



0800-771 5533 — www.unoeste.br

UNIVERSIDADE DO OESTE PAULISTA
UNOESTE
PRESIDENTE PRUDENTE - SP

FIM
Obrigado



PERGUNTAS – DÚVIDAS?

Prof. Dr. Adilson Eduardo Guelfi (guelfi@unoeste.br)
FIPP



0800-771 5533 — www.unoeste.br

UNIVERSIDADE DO OESTE PAULISTA
Unoeste
PRESIDENTE PRUDENTE · SP